NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EMBARKABLES ROOT CAUSE FOR NAVY NETWORKS

by

Noemi Ramirez

March 2012

Thesis Advisor:	John Osmundson
Second Reader:	Weilian Su

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	March 2012	Master's Thesis

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
Embarkables Root Cause for Navy Networks	
6. AUTHOR(S) Noemi Ramirez	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____n/a_____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited	

13. ABSTRACT (maximum 200 words)

Network-centric warfare (NCW) is the Navy's central concept for organizing its efforts to transform itself for military operations in the 21st Century. This concept links together Navy ships and shore sites into highly integrated networks to provide geographically dispersed war fighters and decision makers real-time information exchange at every level.

As the Navy continues its efforts to align network operations, the existing IT structure is falling short in meeting the war fighter requirements. Interoperability among DON networks is critical to improve combat capability and efficiency. Navy war fighters require seamless access to IT services while deployed anywhere in the world. The Embarkables process provides the ability for users to move their workstation between networks but consists of a complex and time consuming IT process when transitioning from shore facilities and to ship environments. This thesis identifies root causes for network interoperability problems faced by embarking units when connecting to alternate networks, in this case the information technology for the 21st Century environment. This thesis also recommends approaches to improve integration of ashore assets into the shipboard environment, and suggests further areas of research for a seamless user experience moving across networks

14. SUBJECT TERMS	15. NUMBER OF PAGES
Navy Marine Corps Intranet (NMCI); OCONUS Navy Enterprise Network (ONE-NET); Information Technology for the 21st Century (IT-21), Embarkables; Deployables; Network Interoperability	133
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

EMBARKABLES ROOT CAUSE FOR NAVY NETWORKS

Noemi Ramirez
Civilian, Department of the Navy
B.S., California Polytechnic State University Pomona, 1999

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
March 2012

Author: Noemi Ramirez

Approved by: John Osmundson, PhD
Thesis Advisor

Weilian Su, PhD
Second Reader

Cliff Whitcomb, PhD
Chair, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Network-centric warfare (NCW) is the Navy's central concept for organizing its efforts to transform itself for military operations in the 21st Century. This concept links together Navy ships and shore sites into highly integrated networks to provide geographically dispersed war fighters and decision makers real-time information exchange at every level.

As the Navy continues its efforts to align network operations, the existing IT structure is falling short in meeting the war fighter requirements. Interoperability among DON networks is critical to improve combat capability and efficiency. Navy war fighters require seamless access to IT services while deployed anywhere in the world. The Embarkables process provides the ability for users to move their workstation between networks but consists of a complex and time consuming IT process when transitioning from shore facilities and to ship environments. This thesis identifies root causes for network interoperability problems faced by embarking units when connecting to alternate networks, in this case the information technology for the 21st Century environment. This thesis also recommends approaches to improve integration of ashore assets into the shipboard environment, and suggests further areas of research for a seamless user experience moving across networks.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACL	Access Control List
AD	Active Directory
AES	Airwing Embarkables Server
ASN	Assistant Secretary of the Navy
BLII	Base Level Information Infrastructure
C4I	Command, Control, Communications, Computers, & Intelligence
CA	Core Application
CAC	Common Access Card
CAE	Client Automation Enterprise
CD/DVD	Compact Discs/Digital Versatile Discs
CIO	Chief Information Officer
CND	Computer Network Defense
COCO	Contractor Owned Contractor operated
CONUS	Continental United States
CSFL	Common Systems Function List
CTO	Communications Tasking Order
DAR	Data at Rest
DHCP	Dynamic Host Configuration Protocol
DIL	Disconnected, Intermittent, Limited
DISA	Defense Information Systems Agency
DMT	Deployables Management Tool
DON	Department of the Navy
DSL	Digital Subscriber Line

DSTB	Deployable Site Transport Boundary
DWM	Deployable Workstation Management
EMS	Enterprise Management System
ePO	ePolicy Orchestrator
ESIT	Embarkables Staff Integration Team
GE	GuardianEdge
GE EA	GE Encryption Anywhere
GERS	GE Removable Storage
GOGO	Government Owned Government Operated
GPO	Group Policy Object
HBSS	Host Based Security System
HBSSMA	HBSS McAfee Agent
HIPS	Host Intrusion Prevention System
IAM	Information Assurance Manager
IAVM	Information Assurance Vulnerability Management
IBM	International Business Machines
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ISNS	Integrated Shipboard Network System
IT	Information Technology
IT-21	Information Technology for the 21st Century
JTF-GNO	Joint Task Force for Global Network Operations
LNSC	Local Network Service Center
MCEN	Marine Corps Enterprise Network
MBR	Master Boot Record

MR	Maintenance Release
NALCOMIS	Naval Aviation Logistics Command Management Information System
NAS	Network Attached Storage Device
NCES	Net-Centric Enterprise Services
NETWARCOM	Naval Network Warfare Command
NMCI	Navy Marine Corps Intranet
ONE-NET	Outside the Continental United States Navy Enterprise Network
OS	Operating System
OU	Organizational Unit
PA	Policy Auditor
PBA	Pre-Boot Authentication
PEO	Program Executive Office
PKI	Public Key Infrastructure
PMW	Program Manager, Warfare
POR	Programs of Record
PPS	Pre-Positioned Servers
PUK	Pack Up Kit
RAS	Remote Access Service
RD&A	Research, Development and Acquisition
RSD	Rogue System Detector
SATCOM	Satellite Communication
SCCM	Microsoft Systems Center Configuration Manager
SCI	Sensitive Compartmented Information
SIDs	Security Identifiers
SME	Subject Matter Experts

TNOSC	Theater Network Operations and Security Center
TWT	Two Way Trust
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WPMS	Windows Patch Management System
WSUS	Microsoft Windows Server Update Services
NOC	Navy Operations Center
ODAA	Office of the Designated Approving Authority
RTT	Round Trip Times
SSO	Single Sign-On

EXECUTIVE SUMMARY

Successful military missions rely on secure, reliable, available communication networks anytime, anywhere. The current Naval networking environment is composed of four enterprise networks (NMCI, ONE-NET, IT-21 and MCEN) supporting over half a million Navy and Marine service men and women around the world executing these missions. These networks are becoming large complex systems with relatively stable architectures, with no standardization of technologies or protocols, with variations of security policies and requirements, and with significant architectural differences resulting in network interoperability challenges, and degradation and loss of communication efficiency of mobile users.

As the Department of Defense (DoD) strives for network commonalty and alignment, immediate capabilities are needed to support deploying forces anywhere in the world. Embarkables provide mobile Navy and Marine assets the ability to integrate into the IT-21 environment for multiple deployment scenarios, but the diversity of operational environments and Embarkables processes result in cumbersome and time consuming integration problems.

This thesis provides an overview of existing Embarkables mechanisms and identifies gaps in IT services and capabilities available to ashore systems while connected to the IT-21 topology. It identifies possible contributing factors to the management deficiency of Embarkables workstations, such as the decentralized network management afloat model, the variation and incompatibility of management tools and the high failure rate of patch downloads due SATCOM constraints.

In additional to the network management interoperability issue, DoD security mandates such as Hosted Base Security System (HBSS) introduce challenges to the integration of ashore assents into the afloat network. Solutions driven by these security mandates include multiple agents managing communication between workstations and policy enforcing servers, client firewalls configured with policies for inbound and outbound traffic specific to each network, and agents to perform scan of configuration

settings. Embarking units cannot access their native network HBSS servers and are not compatible with the ship's HBSS servers and policies. This deficiency requires manual processes to install and uninstall various instances of HBSS.

Active Directory (AD) structures are analyzed to determine how the operational environments and system requirements influenced present architectural designs. Navy ships' operational environment utilizing satellite communication adds the requirement for each ship to be self-sustained while at sea. This decentralized, multi-forest network management model meets its purpose of providing data isolation and prevents network asset mobility or integration from any other domain by preventing any data sharing, replication, and collaboration with other IT-21 ships or with the ashore networks. Alternatively, wired ashore networks offer superior performance and reliability. NMCI and ONE-NET share a similar AD model of a single forest, fully meshed structure allowing continued replication at the enterprise level. This AD structure provides centralized identification and authentication control, allowing user and seat mobility between logical and physical sites.

The author provides recommendations for more efficient and prompt integration of ashore assets into the shipboard environment by (1) testing all ashore solutions against the Embarkables process prior to fielding to the operational environment, (2) adapting existing solutions to provide "office like" services to embarking users such as an enhanced DSTB solution currently accredited and in operation on NMCI, and (3) exploring new technologies such as enterprise services (individually or as a bundle) such as e-mail services, by fully or partially outsourcing these services to a third party.

In summary, the Embarkables mechanisms support the Navy's need to deploy personnel and equipment for military training, humanitarian, and combat mission operations as an interim fix to today's network interoperability issues.

As DoD aligns systems and resources across organizations and military services, enterprise systems must be flexible, adaptable and reconfigurable. Whether developing new solutions or upgrading operational networks, system architects and engineers must implement a system-of-system approach and focus on developing dynamic

reconfigurable system architectures, with standardized protocols and technologies to enable adaptable and interoperable reliable systems to function anytime, anywhere.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

My sincere gratitude to the Naval Postgraduate staff for their support and for the pleasant learning experience provided during the last two years. Very special thanks to my thesis advisor Dr. John Osmundson, and second reader and Dr. Weilian Su for their assistance and guidance provided for the successful completion of this thesis.

I would also like to thank my classmates for the moral support and encouragement; they made this a rewarding learning experience. My deep appreciation to my Command, SPAWAR SYSTEMS CENTER PACIFIC for the opportunity I was given to further enhance my knowledge in the Systems Engineering field and grow as a professional in the DON community. Very special thanks to NMIC, ONE-NET and IT-21 engineers and managers who took the time to provide information and review documents for accuracy.

Con mucho cariño principalmente a mi querida familia por su apoyo incondicional y el estímulo que siempre me brindaron para seguir adelante hasta lograr esta nueva meta. Con amor y agradecimiento infinito, los quiero mucho.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

The concept of Network-Centric Warfare (NCW) is the Department of Defense doctrine for organizing its efforts to transform itself for 21st Century military operations by leveraging technical advances in information technology and telecommunications to improve military operations and increase combat power. The NCW concept links together Navy ships and shore sites into highly integrated networks to provide geographically dispersed war fighters and decision makers real-time information exchange between every level of echelon in the joint military hierarchy needed to effectively execute U.S. military missions (Department of the Navy Chief Information Officer, 2008).

FORCEnet is the Department of the Navy (DON)'s vision of implementing NCW. Its objective is to integrate data, commands and capabilities into a single naval intranet to seamlessly and effectively share tactical information among the afloat and ashore forces. Under the Naval Network Warfare Command (NETWARCOM) governance, the Navy is implementing the FORCEnet doctrine by consolidating legacy networks into highly reliable, more secure centralized networks. Key Navy programs implementing the FORCEnet doctrine are: the Information Technology for the 21st Century (IT-21) program, also known as Integrated Shipboard Network System (ISNS); the Navy-Marine Corps Intranet (NMCI); and the Base Level Information Infrastructure (BLII) Outside the Continental United States (OCONUS) Navy Enterprise Network (ONE-NET). These three networks service most Navy and Marine users in the Unites States onboard U.S. Navy vessels and OCONUS.

As the FORCEnet concept, depicted in Figure 1, continues guiding and shaping the future of naval command and control communications, IT-21, NMCI and ONE-NET networks have linked over 16 major OCONUS Navy sites, 400 CONUS Navy and Marine locations, and almost 200 surface ships. They provide secure and non-secure IT

capabilities and services to over 827,000 users, 375,000 workstations and transport of more than 125 million e-mails each month.

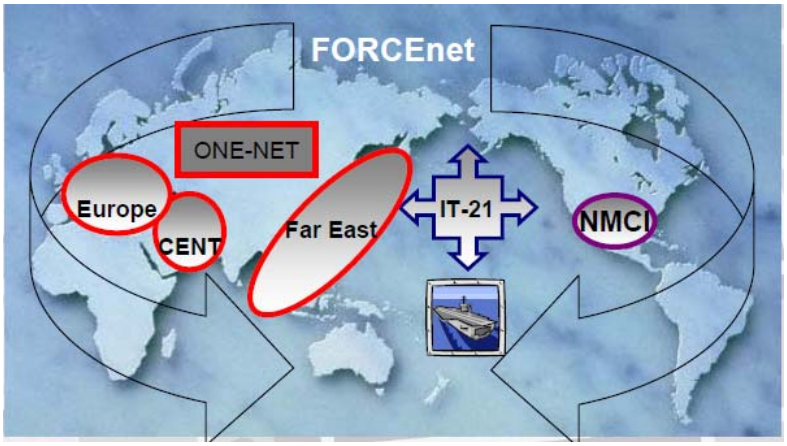

Figure 1. FORCEnet Concept Diagram (From Department of the Navy Chief Information Officer, 2008)

As U.S. military forces deploy every day all around the globe, approximately 100,000 war fighters require reliable network communications and access to IT data and services for efficient military operation support while deployed at any dispersed Navy and Marine location. Interoperability among the three networks is a critical element to provide continuous IT services to deployed units and to improve Navy combat power and information superiority (Runyan, 2006).

There are Navy wide efforts to improve network interoperability, but the immediate need to embark NMCI and ONE-NET systems into the IT-21 environment has driven the emergence of the Embarkables mechanisms currently in operation. These Embarkables mechanisms (also called Deployables) provide the capability for ashore users to move their workstations and data to the afloat environment to receive basic IT services, but the integration of systems into the IT-21 topology involves complex and time consuming IT processes.

The three networks have unique Embarkables requirements and capabilities based on their mission (Rivera, Deployables STEAG Brief, 2009). These high-level Embarkables requirements are summarized below:

- IT-21

- Not required to deploy to NMCI or ONE-NET environments
- Required to support integration of NMIC and ONE-NET users/workstations

- NMCI
  - Requirement to deploy to IT-21 and ONE-NET environments
  - Not required to support integration of ONE-NET or IT-21 users/workstations

- ONE-NET
  - Requirement to deploy to IT-21 environment
  - Required to support integration of NMCI users/workstations

Figure 2 illustrates the high-level Embarkables requirements framework.

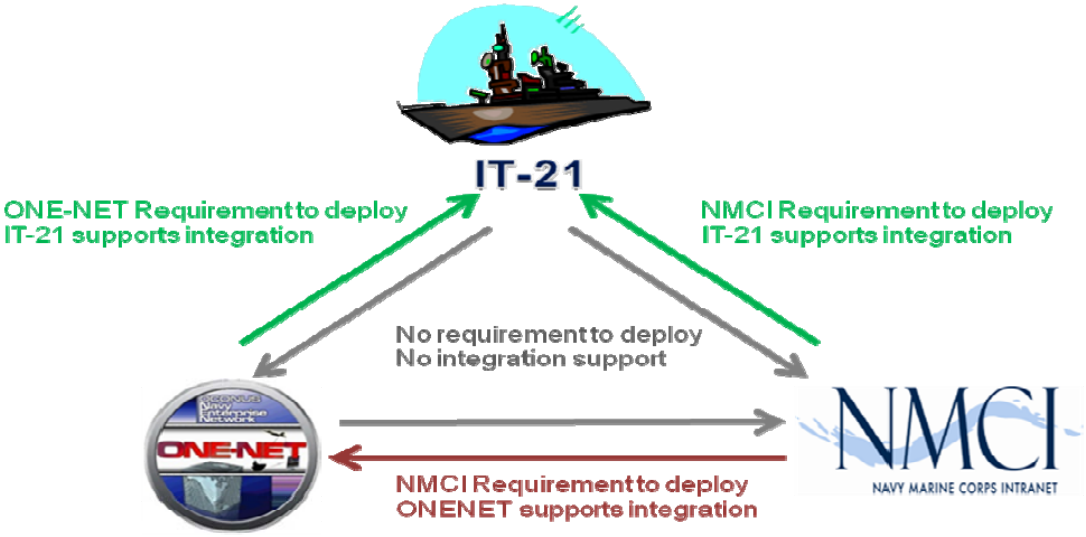

Figure 2. High Level Embarkables Requirements (From Rivera, Deployables STEAG Brief, 2009)

IT-21, NMCI and ONE-NET currently service different regions, operate independently from each other, consist of different architectures, are bound to different security and accreditation requirements, and implement different Embarkables procedures on deployed units. The result is a variation of the Embarkables process and deficiencies across the enterprise.

B. PURPOSE

The purpose of this thesis is to identify the Embarkables operational requirements; investigate the current Embarkables processes, their shortcomings and challenges; and identify potential root causes, technical and/or programmatic, for existing Embarkables issues in order to provide recommendations to improve ashore asset integration into the afloat network, so that embarking staffs and users face a minimal amount of effort and time to access Navy IT resources and services during deployment.

C. RESEARCH QUESTION

The following questions are addressed in this thesis:

- What are Embarkables and what are the challenges they currently face?
- What are the requirements for the deployed users/systems for each network?
- What is the impact of different desktop configurations?
- What are the network management and architecture differences?
- How can the Navy users better and quicker integrate their deployed systems into afloat domains?
- How can the Navy users better and quicker integrate their deployed systems into all Navy domains?
- How can seamless e-mail access be achieved?

D. BENEFITS OF STUDY

The Navy's desired goal is the interoperability of NMCI and ONE-NET embarked users and workstations in the IT-21 environment in order to reduce the required reconfiguration of workstation and network devices, reduce administration overhead and maximize fleet efficiency while assets move between Navy network environments.

This thesis identifies existing Navy mobile user requirements and challenges, provides an analysis of all Embarkables and integration mechanisms in place to integrate ashore assets into the afloat environment, and identifies potential causes for interoperability deficiencies. Identifying potential contributing factors causing integration

problems faced by embarking systems will facilitate the improvement and alignment of current processes to position the Navy so that embarking staffs and users face a minimal amount of effort and time to access Navy IT resources and services in all three environments.

E. SCOPE AND LIMITATIONS

The scope of this thesis is to identify the potential Embarkables root cause problems faced by the NMCI and ONE-NET mobile users and workstations connecting to IT-21 topology.

This study includes an analysis of the current Embarkables processes and identifies each network's organizational goals, operational requirements for mobile users, Embarkables processes and technology gaps including desktop image, network management and architecture differences. Because Embarkables requirements differ for IT-21, NMCI and ONE-NET as depicted in Figure 2, this thesis focuses on the NMCI and ONE-NET requirement to deploy to IT-21, and the requirement for IT-21 to support integration.

F. METHODOLOGY

The methodology used in this thesis research consists of:

- Conduct literature review of IT-21, NMCI and ONE-NET system requirements for deployed systems
- Conduct a review of Embarkables pre-deployment, deployment and post-deployment methods for all three networks
- Perform application and software desktop solution analysis for the three networks.
- Analyze the network management processes including patching and application distribution
- Analyze the three different architectures from a programmatic and technical perspective
- Develop recommendations for common Embarkables process across systems

THIS PAGE INTENTIONALLY LEFT BLANK

II. NETWORKS OVERVIEW AND EMBARKABLES REQUIREMENTS

A. INTRODUCTION

The Department of the Navy continues defining and formulating the necessary steps to achieve a net-centric future for the Naval Networking Environment (NNE) in 2016 while exploring and implementing solutions to resolve existing deficiencies and limitations for mobile users. These efforts have resulted in the implementation of various technical solutions and processes to enable IT services for mobile users connecting across naval network environments.

This chapter provides an overview of the Navy's vision for a highly interconnected enterprise networking capability; a synopsis of the existing networks, their mobile capabilities and requirements; and the existing Embarkables mechanisms to provide IT capabilities to the war fighter.

B. THE NAVY'S VISION

As defined on the NNE's Concept of Operations, NNE "is an iterative set of integrated, phased programs that will guide the DON towards a future net-centric enterprise environment." The NNE and Global Information Grid 2.0 vision for DoD information superiority includes (Enterprise Services Working Group, 2010):

- Single Sign-on
- Anytime Anywhere Access to DoD Networks
- Same e-mail for life (Home Station or Deployed)
- Single DoD Directory (Global Access List)
- Joint infrastructure
- Common DoD policies and standards
- Unity of command

The DON's strategy for the NNE initiative is to align networks across the enterprise, so that in the near future, those networks will be bound by a common

enterprise architecture, standards, and governance. There are several ongoing measures to aid and shape the planning for that future: (1) afloat networks such as IT-21, the Combined Enterprise Regional Information Exchange System–Maritime (CENTRIXS-M), the Sensitive Compartmented Information (SCI), and other legacy networks are being consolidated into the Consolidated Afloat Networks and Enterprise Services (CANES) starting in 2012; (2) legacy ashore networks continue migrating into ONE-NET; and (3) the fusion of NMCI and ONE-NET currently in progress to become the Next Generation Network (NGEN) by 2014. Figure 3 provides a graphical representation of the DON vision for the future of Navy networks including the Marine Corps Enterprise Network (MCEN) not covered in this thesis. The current Navy network environment consists of over 400 decentralized networks supporting over 800,000 users worldwide. In this multiple network environment, network interoperability is nonexistent, information sharing is limited, and resources and assets cannot be shared across networks.

The Navy's vision for a net-centric naval network environment is to consolidate and reduce the number of legacy networks, to increase DoD data sharing, and to increase network interoperability and communication efficiency.

Figure 3. Naval Networking Environment (From Carey, 2010)

C. NETWORKS OVERVIEW

Under NETWARCOM's governance and operation, the Program Executive Offices (PEOs) oversee a portfolio of enterprise-wide IT programs designed to enable common business processes and provide standard IT capabilities to sailors at sea, Marines in the field and their support systems. The PEO for Command, Control, Communications, Computers and Intelligence (PEO C4I) oversees the afloat networks including IT-21. The PEO for Enterprise Information Systems (PEO EIS) oversees the ashore Navy networks NMCI and ONE-NET.

1. IT-21 Network Overview

IT-21 is the Navy's investment strategy for procuring the desktop computers, data links, and networking software needed to establish an intranet for transmitting tactical and administrative data within and between Navy ships (Department of the Navy Chief Information Officer, 2008). IT-21 is a PEO C4I Program Manager, Warfare (PMW) 160 product and it provides reliable, high-speed secret and unclassified network communications to Navy ships. The ship's Local Area Network (LAN) hosts other systems such as Global Command and Control System – Marine Corps (GCCS-M), Naval Tactical Command Support System (NTCSS), Navy Standard Integrated Personnel System (DMS), and few other applications and systems. It enables voice, video, and data transmissions from a single desktop PC, allowing the war fighter to exchange tactical or non-tactical information (SPAWAR, 2011). IT-21 is a dynamic environment and consists of complex security and storage requirements with limited data reach-back access due to low bandwidth capacity. It performs identity management and application integration and can support multiuser workstations with the ability to customize their desktops.

2. Navy Marine Corps Intranet

NMCI is the DON shore-based enterprise network in the continental United States and Hawaii, providing a single integrated, secure IT environment for reliable, stable information transfer in both classified and unclassified environments. Previously owned and operated by contractor Electronic Data Systems (EDS) now Hewlett-Packard (HP), NMCI represents about 70 percent of all DON IT operations and it is the second largest

network in the world. NMCI's implementation in 2001 dramatically improved network security across the enterprise while providing secure and non-secure voice, video, data communication and common computing environment (Department of the Navy Chief Information Officer, 2006).

The NMCI contract ended on September 2010 and it was replaced by the Continuity of Services Contract (COSC). NMCI, now COSC, is a government owned and contractor operated network and it is managed by the Navy's PEO EIS and supported by HP. For simplicity, the term NMCI will be used through this thesis but it also refers to COSC.

3. ONE-NET Overview

ONE-NET extends to most overseas Navy bases, posts, camps, stations, activities, and 14 major locations for an estimated user base of 40,000 Navy uniformed and civilian workforce members, including foreign nationals supporting the Navy facilities or joint military operations (Space and Naval Warfare Systems Center, 2010). It enhances system and software security and improved information exchange capability among users in the OCONUS secure and non-secure environments and tactical/business partners in the deployed forces and Joint environment. Similarly to NMCI, it delivers comprehensive end-to-end information services through a common, secure computing and communications environment on both enclaves. ONE-NET is divided into three regions: Far East, Middle East and Europe. The three regions are logically connected to via the Defense Information System Network (DISN) cloud and have centralized control authority.

D. EMBARKABLES REQUIREMENTS

As U.S. forces deploy around the world, approximately 100,000 war fighters require seamless access to enterprise IT services. Users temporally or permanently move from one Navy network to another requiring continuity in core IT services in order to efficiently support the Fleet. This section investigates user network requirements based on high-level Embarkables requirements discussed in Chapter I and illustrated in Figure 2.

The only documented Embarkables requirements are addressed in the NMCI contract (N00024–00-D-6000) at a very high level, without target or threshold service requirements or key performance parameters. Consequently, business rules had to be developed by the PEOs to establish mechanisms to support embarking units and to provide IT capabilities during deployments (Rivera, Deployables STEAG Brief, 2009). These mechanisms are technical and process workarounds to bridge the architectural and programmatic gaps resulting in Embarkables interoperability. These quick fixes partially alleviate the embarking unit's network communication needs by providing some IT capabilities, but they do not provide seamless mobility between networks.

1. Ashore Networks Embarkables Requirements

NMCI and ONE-NET support a variety of Navy and Marine commands requiring frequent deployments to IT-21 environments. Embarking commands vary in size, deployment duration, and mission. These commands' operations and mission success depend on reliable networks to access critical command and control, combat support and combat service support information in voice, video and data formats while deployed on an IT-21 environment. NMCI and ONE-NET require asset mobility to allow integration into a shipboard network and the ability to reintegrate back into their home network with none or minimal delay or lost of data. Both ashore networks require IT-21 to provide core services for short or extended periods of time during deployments.

In addition to NMCI deploying into IT-21, NMCI requires the capability to integrate into ONE-NET to support Navy and Marine units deployed at OCONUS locations where ONE-NET is the Navy's IT service provider. NMCI is not required to support integration of ONE-NET assets, and therefore ONE-NET users cannot connect to NMCI for services while in a CONUS location. NMCI requires reintegration of its users and workstations returning from IT-21 and from ONE-NET environments.

At this time, ONE-NET does not deploy assets into NMCI but is required to support integration of NMCI assets into its topology for temporary deployments. ONE-NET requires reintegration of its users and workstations returning from IT-21.

NMCI and ONE-NET established unique processes to reintegrate their assets back into the network upon completion of deployment. Reintegration back into NMCI or ONE-NET is beyond the scope if this thesis and will not be further analyzed.

2. Afloat Network Embarkables Requirements

IT-21 does not deploy assets outside its network boundaries, therefore there is no requirement for the ashore networks to support integration of IT-21 assets into their topologies. The few exceptions are VIPs such as the Flag staff who deploy outside the IT-21 environment, but these users are outside the scope of this thesis.

Users who transition from an IT-21 ship to another, or to an ashore Navy network are currently not able to seamlessly transfer their data or e-mail to an alternate network. Any data migration is a manual process using authorized external media. User accounts are disabled and deleted on the IT-21 network, and accounts are created on the new network. This is a troublesome manual process and results in loss of user data and productivity.

Although IT-21 is not required to deploy assets, it is required to support user and seat integration from NMCI and ONE-NET. Marine Corps, Airwings, and other shore command deployments are tied to Navy ship deployments and depend on IT-21 for IT services. These commands require continuity of IT services by maintaining access to end user data, access to local servers and mail files to provide the war fighter communication effectiveness in a mobile environment.

3. Users to Move Seamlessly between Networks

Immediate integration into the afloat network is required for embarking users to efficiently operate onboard a ship. This seamless connection into an alternate network is currently not possible for ashore assets, therefore user IT capabilities must be provided by alternate means. User requirements and services for embarking units while connected to the IT-21 network are undefined. This section attempts to identify the Embarkables user IT capabilities needed while connected to the visitor network by assuming embarking units require the same capabilities they obtain as while they are connected to their native network. Capabilities provided by a home network are set as the baseline requirements

for a seamless transition to the visitor network. This assists identifying the Embarkables deltas and shortcomings by comparing the baseline against what embarking units capabilities received during deployments.

A list of high level capabilities required by the NMCI network to its users is identified in Table 1. As users get deployed and are required to temporarily access the afloat network, most of these capabilities are not immediately restored, are degraded, or completely lost.

NEED ID	USER NEEDS
N1	Cryptographic logon to workstation (cached users)
N2	Domain account
N3	Network access
N4	Send/Receive Email
N5	Attach and open email attachments
N6	Access to Contacts
N7	Access to Native Network Global Address List
N8	Ensure workstation protected from cyber attaches and spam
N9	Shared Calendar
N10	Accessibility to user data and email files on local hard disk such as .pst files as part of user profile
N11	Accessibility to user data and email files stored on the user home drive
N12	Outlook Capabilities (email settings, print styles, email rules and setting, etc)
N13	DOD digital email signature and encryption capability for home network email
N14	DOD digital email signature and encryption capability for host network email
N15	MS Office and Other local DoD approved apps for seat/user
N16	Protected data transmissions
N17	Web access and Cache
N18	Authentication Services—PKI/CAC
N19	OS and application patching
N20	Access to web based applications including certificate-based authentication applications
N21	Native Home drive to view, edit, crate and delete files depending on use access
N22	Native Command shared drive to view, edit, crate and delete files depending on use access
N23	Access to Public Folders
N24	Local and network data integrity
N25	Locate and connect to home and share drives
N26	Seat Local Data storage capacity
N27	Receive administrative policies and user privileges
N28	Security policies applied to account
N29	Application management
N30	Air Card and Wireless capability
N31	Print/Scan/Fax capabilities
N32	Locate and connect to printers
N33	Chat and Instant Messaging (IM)
N34	Access to collaboration tools (i.e. Defense Connect Online (DCO)
N35	Command Document collaboration / Portal (SharePoint)
N36	24/7 Help Desk
N37	Technical support
N38	Capability to create a trouble ticket and check status
N39	Training capabilities
N40	Tech Refresh
N41	HW repair or spares (PUK)
N42	Capability to transfer files
N43	Messaging—Alerts
N44	Secure, available and reliable network connection (99% Service Level Agreement)
N45	Backup and Restore Capability
N46	MAC (Move, Add, Change) Capability
N47	VTC capabilities
N48	Access to IT-21 Global Address List
N49	Access to IT-21 resources such as applications
N50	Ability to store to external media
N51	Produce and Manage Audio and Graphic Media
N52	Disconnect/Log out
N53	Ensure non repudiation
N54	Receive all Computer Network Defense policies and mandates (HBSS/DAR/etc)

Table 1. Embarkables User Requirements Baseline (After NMCI, 2010; NMCI, 2009)

The Navy has deployed some functional Embarkables mechanisms to support embarked units into IT-21 to provide some of the required IT services and capabilities and prevent loss in productivity and inefficiencies in any mission efforts. Such mechanisms are analyzed in detail in the next section.

E. EMBARKABLES MECHANISMS OVERVIEW

Prior to any Embarkables process implementation to integrate ashore assets into the afloat network, users were forced to leave behind all workstations and data storage servers on their native network, as those devices were not allowed to connect to the afloat network. As a result, access to users' locally stored data and on shared network drives were not possible, requiring users to export all data into an external media (portable hard-drives, thumb drives, CDs) and carry onboard. E-mail files, user data and command shared data were not accessible during a deployment.

In order to provide basic IT services, ships' staff was required to create user domain accounts as for any other ship user. Hundreds of workstations had to be provided and maintained throughout the deployment period to support the embarking users. Upon completion of the deployment, all accounts were disabled and data created during the deployment transferred via an external media, or left behind and lost. This labor intensive process had to be repeated during every deployment.

The Embarkables process (also known as Deployables) was established to support the Navy's need to deploy personnel and equipment for military training, humanitarian, and combat mission operations as an interim fix to a more complex effort to align Navy networks. IT-21 currently supports embarking groups which vary in size, sometimes over 900 users are deployed to a single carrier adding logistical challenges to provide workstations and IT support for large amount of users.

1. IT-21 Embarkables Mechanisms

IT-21 must support prompt integration of non IT-21 assets into its topology during deployments. Embarkables processes and mechanisms are implemented to integrate and support Navy and Marine embarking units for various scenarios.

U.S. Marine Corps deploy on amphibious warfare ships and aircraft carriers. IT-21 and the USMC have permanently installed Pre-Position Servers (PPS) connected to the IT-21 topology as part of the Ship's domain. Other scenarios involve Navy units embarking onboard IT-21 platforms bringing their own network storage servers, or single users with or without their workstations. These scenarios and the mechanism used for each are described in the following sections.

2. NMCI Deployables Mechanisms

NMCI employs various technical solutions across the enterprise to support NMCI users anywhere in the globe. These solutions include: Two Way Trust (TWT) between NMCI and ONE-NET; Deployable Site Transport Boundary (DSTB) Core; DSTB Fly Away Kit process; NMCI Deployables to IT-21, and current efforts for a Seamless Trust between NMCI and IT-21. Although not all mechanisms are employed on the IT-21 environment, an overview of each of the NMCI deployables solution is provided below:

a. Two Way Trust between NMCI and ONE-NET

The AD two-way-trust between NMCI and OCONUS' Navy networks enables users in either network to access shared resources and enables roaming users to reach back to their home network from the partner network. Through a trust, one partner can share its resources with users native to partner's authentication infrastructure, avoiding the need to create separate accounts. This solution supports interoperability between NMCI and ONE-NET and is therefore outside the scope of this thesis.

b. Deployable Site Transport Boundary (DSTB) Core

The DSTB, also called "NMCI in a box," provides office-like connectivity to NMCI assets while connected to a non-NMCI environment. It allows a small network footprint to reach NMCI resources from the field. The number of users it can support depends on the Wide Area Network (WAN) bandwidth and switch port capacity. It provides versatile WAN connectivity options: T1 (1.544Mbs), Digital Subscriber Line (DSL), Ethernet (10Mbs), ISDN (128K), Fiber (OC3–155Mbs). This capability allows all NMCI assets to operate seamlessly while connected to a host network. It is used for

transport services only, with minimal reconfiguration needed to integrate into the host network's topology. The DSTB architecture consists of an inner router for LAN access, an outer router for WAN access, a VPN device to establish an encrypted tunnel back to the NMCI network, and a WAN accelerator for traffic prioritization and bandwidth optimization.

DSTB provides IT services by local NMCI servers along with an appropriately security enforced backend connection to the host network for needed file, print, app, and web services. All network management functions are available via the Virtual Private Network (VPN) tunnel as illustrated in Figure 4. DSTB provides access to the NMCI network but does not provide access to the host network's resources.

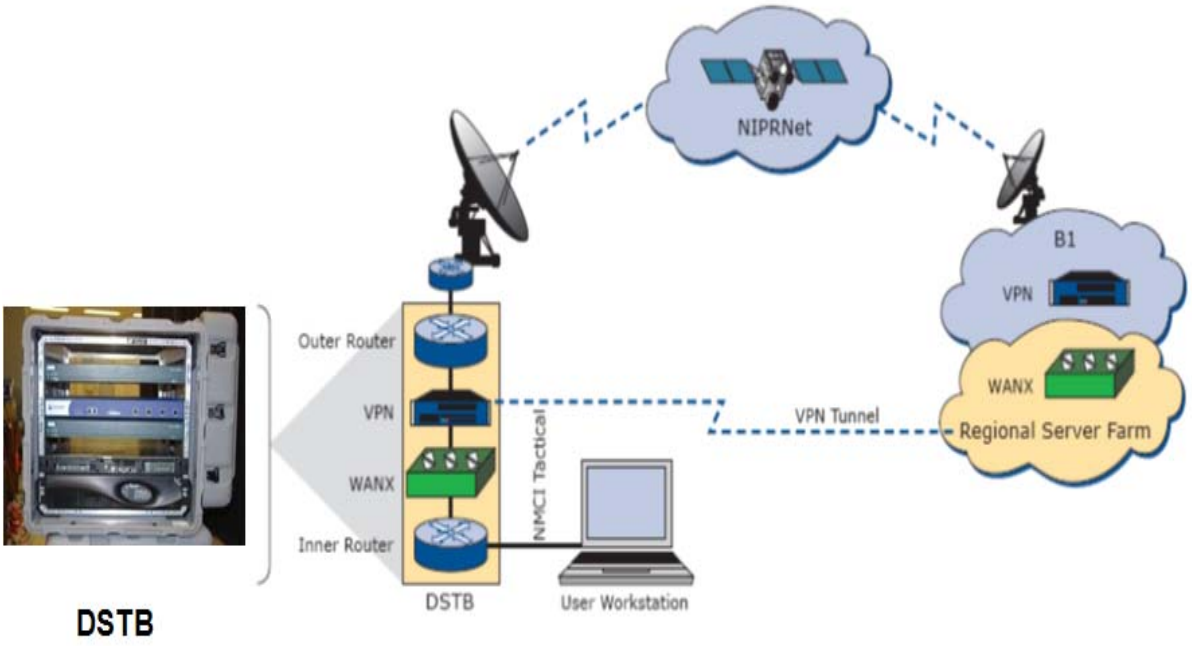

Figure 4. DSTB Architecture (From Hewlett-Packard Development Company, 2010)

c. Deployable Site Transport Boundary Fly Away Kit

Fly Away Kit is the downsized version of the standard DSTB and supports 2–12 users and is mostly use for VIP personnel.

d. NMCI Deployables to IT-21

The objective of the deployables process is to provide operational units the ability to be self-sufficient while in a deployed status on an IT-21 environment. This mechanism is implemented on the unclassified network and it allows embarking ashore personnel to utilize the host environment's network backbone to perform their mission.

U.S. Marines frequently embark on Navy ships to conduct operations from beyond territorial waters. Some Marine fixed-wing squadrons are assigned to Carrier Airwings or amphibious warfare ships to train and operate along with Navy commands. These platforms have pre-deployed server equipment already installed and configured to support embarked Marine units. These PPS suites are installed on a separate domain structure with a two way trust to the ship's domain within the same forest topology, allowing access to the ship's server resources. The embarking unit is responsible for providing and maintaining workstations and performing all domain and user accounts related activities. The required servers to support this host domain can be provided by the ship or augmented by the embarking group.

e. Seamless Trust between NMCI and IT-21

This solution has not been implemented and is under analysis. This solution is intended to establish a trust across NMCI and IT-21 organizational boundaries. This will require a trust between each IT-21 ship (almost 200) to NMCI, resulting in intensive personnel management of all system administrators, restrictions and strictly enforced levels of access of all administrators. This project is currently under evaluation by the PEO's.

3. ONE-NET Deployables Mechanisms

ONE-NET has implemented two technical solutions across the enterprise to support ONE-NET users deployed to NMCI and IT-21 environments. These solutions include: Two Way Trust between NMCI and ONE-NET, and the ONE-NET deployables solution. An overview of each solution is provided below:

a. Two Way Trust between NMCI and ONE-NET

The two-way trust between the ashore networks was described in Section 2.a in this Chapter.

b. ONE-NET Deployables to IT-21

PEO EIS Embarkables solution, also referred to as ONE-NET Deployables, allows deployment of both personnel and equipment outside the ONE-NET environment while providing commands the ability to integrate into the shipboard networks to obtain IT services (ONE-NET does not deploy to an NMCI environment). It supports entire commands or individual users with the primary users being the AIRWINGs in the Far East. This is the process of interest for this thesis as it is implemented for ONE-NET users integrating into IT-21 environments.

During an Embarkables event when ashore users are deployed to the ashore network, IT-21 must successfully and timely perform certain actions to ensure the deployed elements have access to critical combat support, and combat service support information immediately after deployment beings.

F. DEPLOYABLES (EMBARKABLES) PROCESSES TO IT-21

One of the current Embarkables shortcomings is the variation of Embarkables processes followed by the various deployers. These variations result from the different organizational requirements to deploy, the size of the deploying unit and the home network the unit belongs to. This section analyzes the NMCI and ONE-NET Embarkables process for embarking units brining their own pre-position servers onboard and establishing a trust with the ship's network.

1. NMCI Embarkables Process for Large Deployers

The NMCI Deployables Process consists on the creation of a visitor domain on the IT-21 environment and leveraging the automatic transitive trust with the ship's domain for transport services off the ship's boundary. The deployables domain connects to the unclassified LAN on the same Virtual Local Area Network (VLAN) as the ship

assets, and the deployables traffic is routed via the WAN router to the shore NOC. This WAN connection is shared with other IT-21 traffic including CENTRIXS, secret and SCI data as depicted in Figure 5.

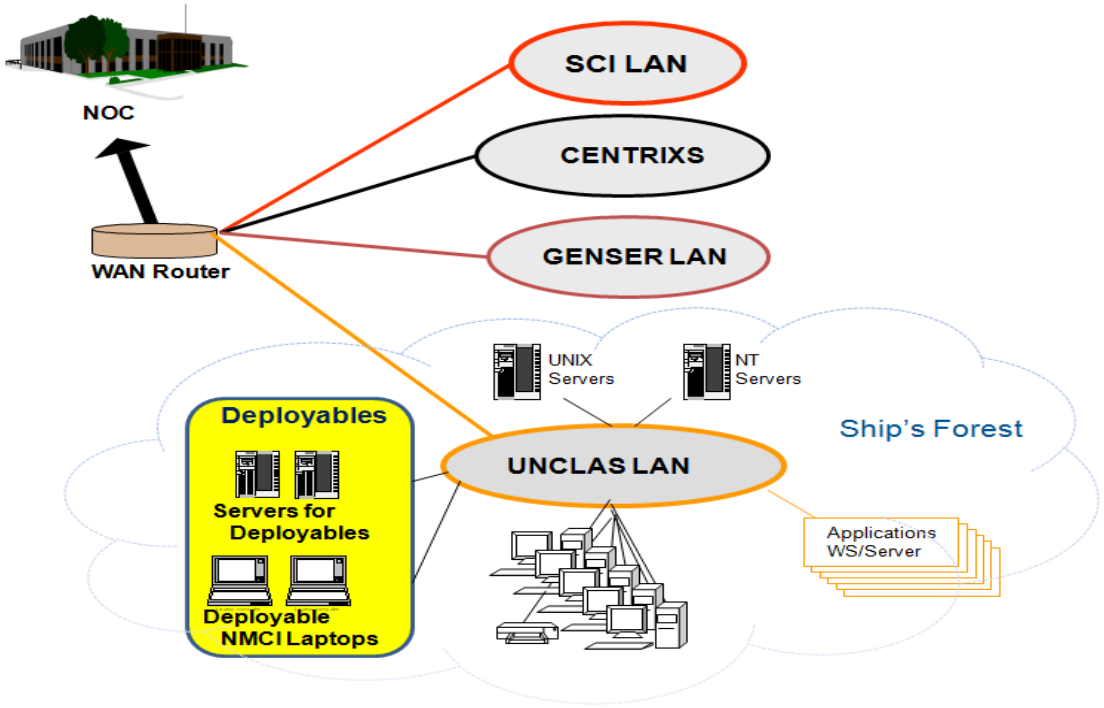

Figure 5. NMCI Connection to Afloat Network (From Smith, 2003)

The deployables solution was engineered for the enterprise but it is primarily used by the large deployers since it requires an Embarkables server suite and IT personnel to support the embarking assets throughout the duration of the deployment. A high level step-by-step Embarkables process is illustrated in Figure 6 and explained in more detailed in following subsection and in Table 2. Pre-deployment step-by-step process for NMCI Embarkables

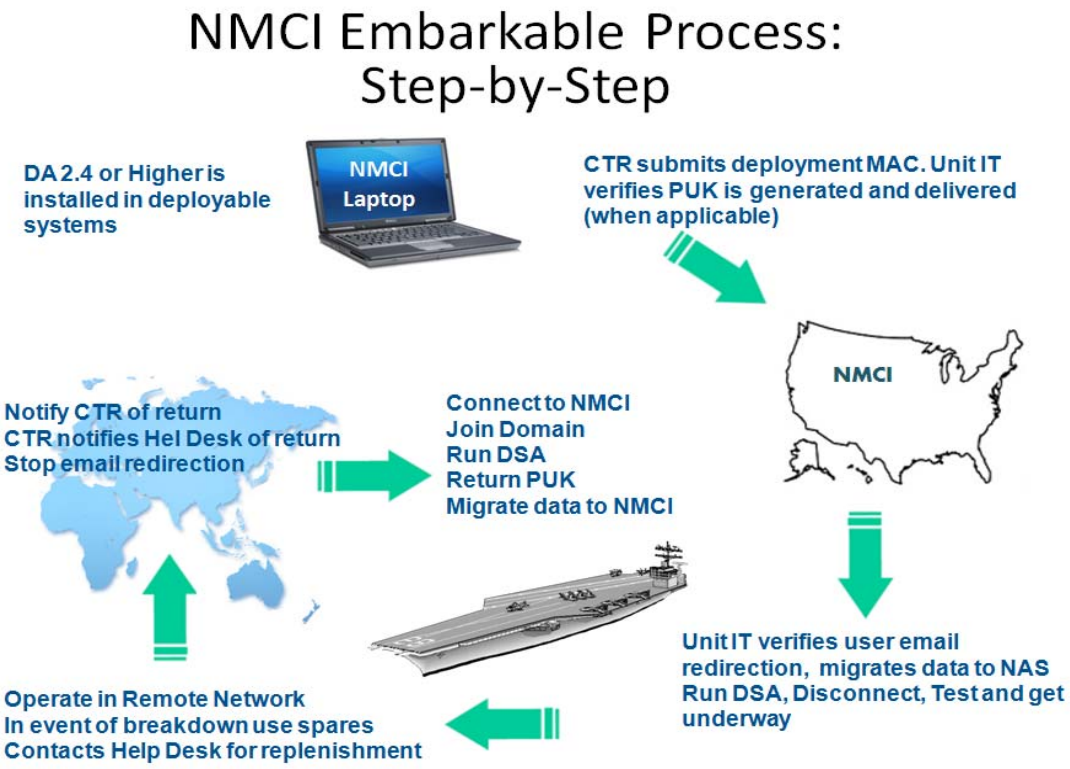

Figure 6. NMCI Embarkables Process: Step-by-Step (From Rivera, Deployables STEAG Brief, 2009)

Pre-Deployment Process: It is the embarking unit's responsibly to plan for a deployment and initiate the Embarkables process by submitting an Embarkables Move/Add/Change (MAC) and requesting ODAA approval to connect to the IT-21 network. Upon completion and approval of a Memorandum of Agreement defining roles and responsibilities between the ship and the embarking unit, the Unit IT requests all required administrative passwords, a Pack-up-Kit (PUK) with a copy of the gold disk and authorized applications, and verifies the availability of an Embarkables PPS suite for their use onboard the IT-21 environment. The Embarkables Staff Integration Team (ESIT) works with the Unit IT to ensure proper hardware and software configuration and functionality of embarking users and workstations.

Typically, the Embarkables servers suite components consists of three (3) servers (Primary Domain Controller (PDC), Backup Domain Controller (BDC), Exchange (EX1)), two (2) Direct Access Storage (DAS) devices, and a Network Access Storage/

Network Fiber Attached Storage (NAS/FAS) device, with two (2) continuous uninterrupted power supply units that are attached to the IT-21 backbone switches (Program Executive Office C4I, 2003). The NAS/FAS device's function is to support the large number of deployable unclassified seats and users associated with the embarking unit and to provide the same storage capability as while connected to the ashore network.

To mirror the IT-21 servers' configuration, the Embarkables servers are loaded with the Common PC Operating System Environment (COMPOSE) load as a POR baseline with the latest security patches and anti-virus definitions. The embarking Unit IT is provided with all needed administrative rights on the IT-21 network to facilitate integration, administer the Embarkables machines, support sustainment and operation during deployment, and to accelerate re-integration back to the native network upon completion of deployment.

The core of the NMCI Embarkables mechanism are the Deployables Application (DA) and the Deployables Management Tool (DMT) for embark capable seats and users. DA is installed on the workstations to perform the background processes for deploying computers. DMT performs background communication with the NMCI Domain Controllers, SQL and Exchange servers via Remote Procedure Call (RPC) and automates the preparation of users and computers by establishing administrative credentials for use during deployment and adjusts state of network dependant services only (workstation modification is limited to avoid costs associated with reconnecting the workstation to the network as users disembark). It suppresses the Enterprise Management System (EMS) functionality on the deploying seat by disabling services which broadcast out to NMCI servers. It turns off all "noisy" enterprise management applications and prepares seats for integration into shipboard Embarkables network. It disables the Information Assurance (IA) and EMS agents which remain inactive for the duration of the deployment (Navy Marine Corp Intranet, 2005). Disabling HBSS is not currently performed by DMT and it remains a manual process.

The following list of applications and services are disabled on each workstation by the DMT in preparation for deployment:

- Computer Browser (Proxy server)
- CPR Loader
- Enterprise Security Agent
- Intruder Alert Agent
- Radia Notify
- Radia Scheduler
- Radia MSI Redirector

DTM enables the following SAV (Symantec antivirus) services on each client:

- DefWatch
- Norton Antivirus Client

Table 2 provides the required actions to be executed (prior to embarkation to the IT-21 environment) by the user, the help desk, or by an authorized system administrator for Marine units leveraging the ship's PPS (Burgard, 2011):

Action ID	ACTION
1	Host domain is created on IT-21 and registered at the NOC.
2	Validate PPS suite connection to the IT-21 environment.
3	Exchange, Domain controllers and DNS servers on PPS are configured.
4	Validate TWT between ship's domain and Embarkables domain.
5	User accounts are created on PPS Primary Domain Controller (PDC)
6	User copies PC data into external media or on their home drives for migration
7	DMT disables IA and network management agents on workstation
8	Email is configured for redirection from the native network to user's IT-21 email address by the help desk or by each user using the DTM tool.
9	Windows printing service is integrated with the Ship's Active Directory
10	NMCI objects from existing Organizational unit (OU) structure in AD are moved to a parallel deployed OU structure on the NMCI AD structure.
11	Workstations from ashore networks with non-COMPOSE image, are connected directly into the IT-21 LAN and joined to the domain. Note: Workstations are not reimaged prior to connecting into IT-21
12	LAN and Outlook settings on workstations are pointed to the PPS suite.
13	IT-21 pushes HBSS agent and HIP to manage HBSS policy during deployment
14	Web Browser settings on all workstation are configured to point to the shipboard Proxy Server and allow for internet access.
15	NMCI Symantec Antivirus clients are redirected to the Symantec antivirus Server on the PPS.
16	Command and users home drives are created on the PPS.
17	Command data and user Home drive data on NMCI storage devices are migrated to NAS prior to embarkation.
18	Back up schedules for PPS and NAS/FAS are verified.
19	A Pack Up Kit (PUK) is obtained and carried onboard for spares and break/fix instructions.
20	A consolidated Information Systems (IS) Help Desk is established for break/fix issues between the ship's help desk and the unit's IT staff.
21	Additional workstations, networks drops, IP addresses are coordinated with IT-21 network system administrator.

Table 2. Pre-deployment step-by-step process for NMCI Embarkables (From Burgard, 2011 and Navy Marine Corps Intranet, 2010)

The ESIT continues supporting the deploying unit from ashore and throughout the duration of the deployment. ESIT ensures the NOC is correctly relaying e-mail to the Deployable domain; maintains and develops documentation and deployment plans and methods for each type of embarkation model; and provides support to the deployed unit as needed via e-mail, phone, or onsite tech assist to resolve critical issues.

During Deployment: During an Embarkables event, NMCI provides the following services to embarked units outside the NMCI environment as specified in the NMCI contract (Navy Marine Corp Intranet, 2005):

- Reachback
- Data Migration
- E-Mail Redirection
- Troubleshooting for Deployed Seats
- Logistics for Deployed Seats
- Training

The non-NMCI network service provider such as IT-21 provides the following services and capabilities (Navy Marine Corp Intranet, 2005):

- Internet Protocol (IP) based communications support
- Data aggregation at local (unit LAN) level
- Information Assurance (IA)
- Data storage at the deployed location
- Security
- System Management
- Legacy Applications Support
- Preferred Publication List (PPL) certification support
- Data Migration/Retention
- Web Access
- File and Print Services
- Directory Services
- E-mail (Hosting)

A local administrator password is issued to the Unit IT for each deployment. The Unit IT is responsible for maintaining the Embarkables servers and workstations to its home network's baseline, including up-to-date security and administrative policies by performing all maintenance and break fix activities on the embarked units including but not limited to following list in Table 3.

Action ID	ACTION
1	Ensuring antivirus updates are being pulled and GAL synchronization on domain exchange servers
2	Ensuring all applicable IAVA patches are applied to all workstations
3	Ensuring all machines have the latest anti-virus definitions.
4	Maintaining seat(s) operational functionality
5	Ordering and managing spares replacements
6	Rebuilding any seat(s) as necessary utilizing the Break Fix tool and process
7	Enforce configuration management of embanked systems
8	Ensuring all installed infrastructure and equipment is maintained within configuration standards
9	Performing Full System Backup of the NAS.
10	Providing technical support for embarked assets

Table 3. During deployment User IT responsibilities (From Navy Marine Corps Intranet, 2010)

In this state, workstations have the networks management agents disabled and can no longer connect to NMCI. User accounts remain active throughout the duration of the deployment and user e-mail is redirected to the IT-21 address.

Post-Deployment: Upon completion of the deployment, the process is inverted in order to reintegrate into the native network. Post deployment processes are dependent on the command policies and regulations to reconnect to the home network.

The Unit IT must re-baseline the workstations prior to integration back to the home network. IT-21's HBSS is removed for NMCI seats and POR Servers; Retina scans on NAS/FAS are performed and discrepancies are remediated; Unit IT must remove any installed applications (licensed or unlicensed application) before re-entering to the NMCI domain. Due to the complexity of bringing each workstation up its NMCI baseline, especially if applications were loaded and proper patching was not performed during deployment, some commands opt out to reimage the workstations prior to ashore integration. Post-deployment processes and issues are addressed locally by the native network staff, and are outside the scope of this thesis.

2. ONE-NET Embarkables Process for Large Deployers

The ONE-NET Deployables process was developed to integrate and support users using a similar process to the NMCI process currently used by the IT-21 staff and ESIT

personnel. ONE-NET most frequent embarking units are the Airwings in Japan. These embarking units are integrated into an Embarkables forest and connected to the unclass LAN topology as depicted in Figure 7. An AD two-way-trust is manually established between the Embarkables forest and the ship's forest for transport services to the shore NOC and to leverage ship resources. ONE-NET Embarkables traffic shares WAN the links with the secret and SCI traffic back to the NOC.

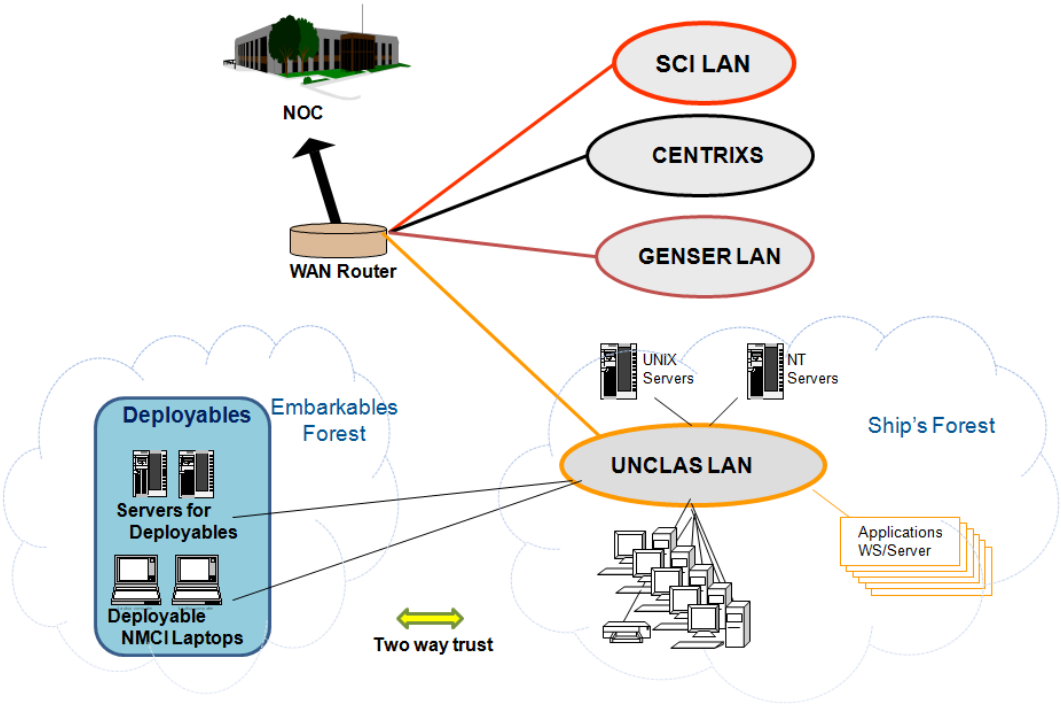

Figure 7. ONE-NET Connection to Afloat Network (From Smith, 2003).

The current ONE-NET Embarkables process largely mirrors the existing NMCI deployable process in order to gain efficiency, commonality and standardize the process, hardware and training. Figure 8 illustrates the ONE-NET high level deployables process.

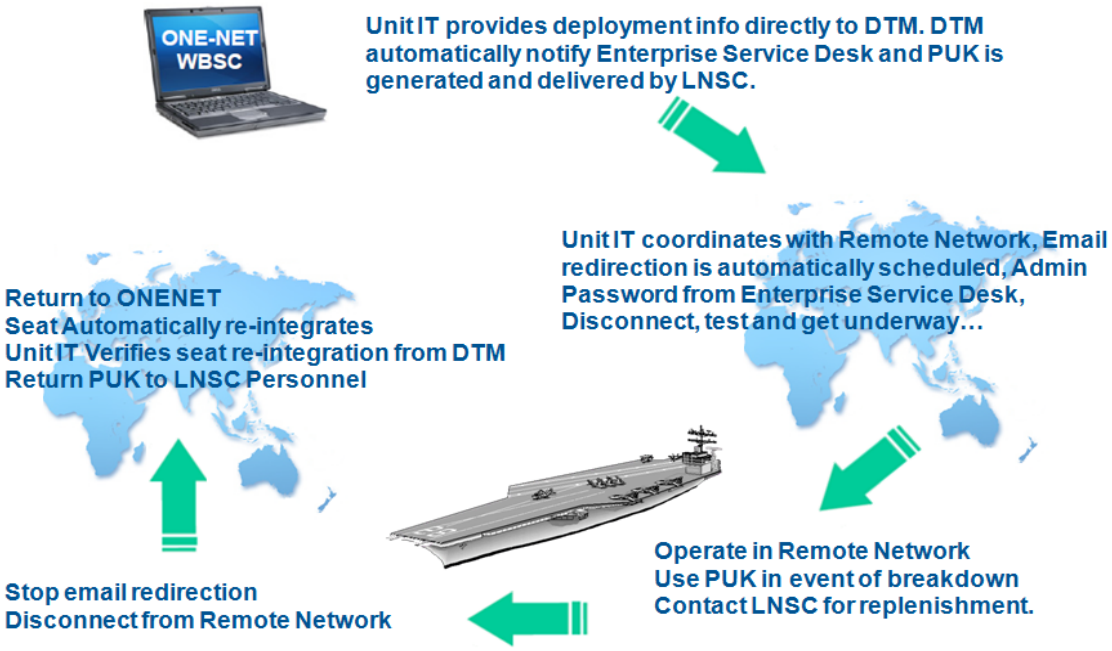

Figure 8. ONE-NET Embarkables Process: Step-by-Step (From Rivera, Deployables STEAG Brief, 2009).

Similarly to NMCI, ONE-NET Deployables is comprised of DMT, hardware assets, spares, and documentation which describes the roles, responsibilities and actions required to support deploying assets. The DMT design supports NIPRNet and SIPRNet environments and requires approval authority by the ODAA.

Pre-Deployment: The process initiates by the Information Assurance Manager (IAM) appointing a Unit IT who is responsible for properly managing the deployment process from beginning to end. OCONUS commands coordinate deployment with the Local Network Service Center (LNSC) or Theater Network Operations and Security Center (TNOSC).

Users to be deployed are identified and are issued a seat capable of deploying. The deployment is then scheduled using the DMT for e-mail redirection and to prepare the workstations to a deployable state. DMT places computer objects into a windows security group upon deployment date. Members of this security group receive the Internet Protocol Security (IPSEC) workstation policy GPO which restricts network access, only allowing communication to Domain Controllers (join workstation to domain, Dynamic

Host Configuration Protocol (DHCP)), Tivoli (Scans, Patching), Symantec (Antivirus definitions) as well as the DMT Server on the date set for deployment.

DMT adjusts the state of network dependant services, such as disabling or turning off services broadcasting out looking for ONE-NET servers. The list of these services is constantly modified based on the ONE-NET baseline updates and includes the following services (Space and Naval Warfare Systems Center, 2010):

- Computer Browser (Proxy server)
- Tivoli Management Agents including remote control and endpoint
- Windows Firewall/Internet connection sharing
- Symantec's Antivirus Endpoint Protection (SEP) 10.1.9
- Exchange export fields
- IPSec policy to restrict access during reintegration
- Password associated with deployed administrative credentials

The following steps listed in Table 4 are executed by the user, the help desk or by an authorized systems administrators and aided by the LNSC or TNOSC:

Action ID	ACTION
1	Host domain is created and IT-21 and registered at the NOC.
2	If command embarking with PPS, the server suite is connected to the IT-21 unclass LAN
3	An Embarkables forest is created following the ship's naming convention
4	A TWT is established between IT-21 and the visiting domain.
5	User domain accounts are created on PPS, including email
6	User copies PC data into external media or on their home drives for migration
7	DMT disables IA and network management agents on workstation, except HBSS
8	Email is configured for redirection from native network to user's IT-21 email address as bulk by the Unit IT desk or each user using the DTM tool.
9	Exchange, Domain controllers and DNS server are configured to point to the ship's servers
10	Windows printing service is integrated with the ship's Active Directory.
11	ONE-NET objects from existing Organizational unit structure in AD are moved to a parallel deployed OU structure in AD
12	A hidden AD contacts with all existing user information (phone numbers, display name, etc) is redirected using the email address as a custom recipient address.
13	LAN and Outlook settings on workstations are pointed to the PPS suite.
14	Workstations with ONE-NET baseline image are connected directly into the IT-21 LAN and joined to the ISNS domain.
15	Web Browser settings on all workstation are configured to point to the shipboard Proxy Server and allow for internet access.
16	Symantec Antivirus clients are redirected to the Symantec antivirus Server on the PPS.
17	Command and users home drives are created on the PPS
18	Command data and user Home drive data on NMCI storage devices are migrated to PPS NAS prior to embarkation.
19	Back up schedule for PPS and NAS are verified.
20	A Pack Up Kit (PUK) is obtained
21	A consolidated Information Systems (IS) Help Desk with the ship's help desk is established for break/fix issues.
22	Additional workstations, networks drops, IP addresses are coordinated with IT-21 network system administrator (PEO-EIS, 2010).

Table 4. Pre-Deployment step-by-step process for ONE-NET Embarkables (From Burgard, 2011)

At this state, deployable computers have limited access to the home network for the duration of the deployment but ONE-NET accounts would remain active as users were coming back. A local administrator password is issued to the Unit IT for each deployment. The Unit IT is responsible for maintaining the Embarkables servers and workstations to the ONE-NET baseline and for properly executing the activities required during deployment as listed in Table 3.

3. Shortcomings for the Existing Embarkables Process

As DoD forces continue deploying all around the world, the existing NMCI and ONE-NET Embarkables mechanisms provide embarked users some of the required IT capabilities, but gaps exist, resulting in an impact to the embarked unit's readiness and efficiency. Some of these gaps or additional labor intensive activities are derived from process differences. Although the Embarkables process was established to support all users at the enterprise, the primary users are large deployers such as Marine Units and Airwings. Single users and small groups who do not normally deploy are not familiar with Embarkables process; their Unit IT(s) do not receive the proper training and are not aware of the Embarkables tools available to facilitate a smooth deployment such as the ESIT support and the PPS capabilities (Embarkables Staff Integration Team , 2008). The following are some variations of the Embarkables Process for large deployers:

- ONE-NET and NMCI have different variation of DTM tools and capabilities. NMCI tool provides Unit IT less visibility and control to manage the deployment vice ONE-NET tool.
- IT-21 provides PPS for Marines on large platforms but Airwings are bringing their own AES and PPS servers. Instructions and configuration settings for command provided PPS are provided by the ESIT but due to the variation of possible configurations, additional work and troubleshooting is required to integrate the PPS into IT-21.
- Each network has different security requirements enforced by ODAA which result different firewall settings.
- Re-integration to the native network process varies depending on the security requirements set for each network and the policies specified by the network's organization.
- Users or small commands without access to PPS or NAS devices cannot leverage these capabilities and therefore are directly connected to the IT-21 LAN as a host client.

In addition to process differences, gaps on services and capabilities received by the embarked units vary depending on the network they are coming from, the amount of users in the embarked unit and the Embarkables mechanism used. These gaps are identified by analyzing what is currently provided by the home networks as described in Table 1 and comparing to services and capabilities obtained by the embarked units on IT-

21 environments using the Embarkables process. Three user cases are defined and analyzed to identify gaps in services received while deployed:

User Case 1 –Airwings, Marine or any other command user on a host domain riding the ship's network for transport services and for minimal access to ship resources. The command is on its own domain connected to the Ship's LAN as depicted in Figure 5 and Figure 7 with a two way trust with the ship's domain. The AES, Pre-Position Servers including the NAS devices for data migration are available. DMT is used to prepare workstations and disable services previously listed. User e-mail is re-directed to an IT-21 e-mail by the user, the Unit IT or the help desk. Mechanism used: NMCI Deployables process

User Case 2 – Single or Small group of NIPR users directly connecting to IT-21 ISNS LAN for all IT services on a small platform. Embarked users bring their home network deployable workstations, but ship or command does not provide PPS or NAS capabilities. DMT is used to prepare workstations and disable services preciously listed. User e-mail is re-directed to an IT-21 e-mail by the user, the Unit IT or the help desk. Mechanism used: NMCI Deployables Process

User Case 3 – NIPR User connecting directly to the IT-21 network for all IT services. User is deployed without a deployable workstation or laptop and will require an IT-21 provided seat for network access. This user case represents the single or small group of users having to embark on an IT-21 environment or those Commands who not normally deploy and is not familiar of the process. User ashore e-mail is not redirected to the IT-21 e-mail, but can be accessed via Outlook Web Access. Mechanism used: User is added to IT-21 topology under Embarkables OU.

Evaluating the services and capabilities obtained during an Embarkables event by each of the three User cases described above, and comparing to User requirement identified in Table 1, gaps in capabilities were identified and summarized in Table 5. User needs colored in red represent unmet needs during an embarkation. Yellow fields represent those needs requiring additional reconfiguration to the network prior to

Embarkables integration. Green fields represent the needs that seamlessly provided by the host network and/or capabilities provided by using the PPS and NAS.

NEED ID	USER NEEDS	User Case 1	User Case 2	User Case 3
N1	Cryptographic logon to workstation (cached users)			
N2	Domain account			
N3	Network access			
N4	Send/Receive Email			
N5	Attach and open email attachments			
N6	Access to Contacts			
N7	Access to Native Network Global Address List			
N8	Ensure workstation protected from cyber attaches and spam			
N9	Shared Calendar			
N10	Accessibility to user data and email files on local hard disk such as .pst files as part of user profile			
N11	Accessibility to user data and email files stored on the user home drive			
N12	Outlook Capabilities (email settings, print styles, email rules and setting, etc)			
N13	DOD digital email signature and encryption capability for home network email			
N14	DOD digital email signature and encryption capability for host network email			
N15	MS Office and Other local DoD approved apps for seat/user			
N16	Protected data transmissions			
N17	Web access and Cache			
N18	Authentication Services—PKI/CAC			
N19	OS and application patching			
N20	Access to web based applications including certificate-based authentication applications			
N21	Native Home drive to view, edit, crate and delete files depending on use access			
N22	Native Command shared drive to view, edit, crate and delete files depending on use access			
N23	Access to Public Folders			
N24	Local and network data integrity			
N25	Locate and connect to home and share drives			
N26	Seat Local Data storage capacity			
N27	Receive administrative policies and user privileges			
N28	Security policies applied to account			
N29	Application management			
N30	Air Card and Wireless capability			
N31	Print/Scan/Fax capabilities			
N32	Locate and connect to printers			
N33	Chat and Instant Messaging (IM)			
N34	Access to collaboration tools (i.e. Defense Connect Online (DCO)			
N35	Command Document collaboration / Portal (SharePoint)			
N36	24/7 Help Desk			
N37	Technical support			
N38	Capability to create a trouble ticket and check status			
N39	Training capabilities			
N40	Tech Refresh			
N41	HW repair or spares (PUK)			
N42	Capability to transfer files			
N43	Messaging—Alerts			
N44	Secure, available and reliable network connection (99% Service Level Agreement)			
N45	Backup and Restore Capability			
N46	MAC (Move, Add, Change) Capability			
N47	VTC capabilities			
N48	Access to IT-21 Global Address List			
N49	Access to IT-21 resources such as applications			
N50	Ability to store to external media			
N51	Produce and Manage Audio and Graphic Media			
N52	Disconnect/Log out			
N53	Ensure non repudiation			
N54	Receive all Computer Network Defense policies and mandates (HBSS/DAR/etc)			

Seamless or provided by PPS and NAS
Provided by the IT-21 environment
Not available

Table 5. Embarkables Requirements Deltas

While embarked units such as users in Case 1 appear to have few seamless capabilities, these are due to the PPS and NAS for the most part. Once workstations are added to the ISNS domain, local user profiles and data can only be accessed by system administrators, therefore users have no access to their locally stored data once they are joined to the domain as their workstation becomes part of the COMPOSE environment.

E-mail redirection allows users to have all e-mails received on their native network e-mail address to be forwarded to their IT-21 mailbox after Microsoft Outlook settings have been reconfigured to point to the ship's exchange servers. E-mail not set for redirection can be accessed via web using the proper credentials to authenticate the same way it can be accessed from a home network, via web access and with the proper user authentication. This requires users to have their CAC capable seat on the IT-21 network and proper credentials to authenticate and access their native network to retrieve e-mail.

Any network storage capability such as home drive and command shared data is only available when PPS and NAS are used and data is migrated to these devices prior to deployment. Network operation and management activities are supported by the Unit IT staff for large deployers bringing an Embarkables server suite or by the ship's staff for small deployers. Users without Unit IT support fully depend on the ship's staff to integrate into IT-21.

G. CHAPTER SUMMARY

Existing Embarkables mechanisms have improved the way embarked units perform their operations during deployment but still some shortcomings exist. The existing NMCI and ONE-NET Embarkables processes share a level of commonality especially for connection to IT-21, but the lack of defined and approved enterprise Embarkables requirements, inconsistencies in Embarkables processes, and difference in network policies lead to variation of these Embarkables capabilities and gaps.

This chapter identified IT capability gaps faced by users in embarking different scenarios. Based on the analysis, it is evident that there is a lack of network interoperability between ashore and afloat networks. The use of PPS and NAS provide many of the needed capabilities to large deployers, such as Marine units and Airwings,

but there no solution available for small units or single users who do not usually deploy, or for smaller decks who might need to support small group of ashore users.

Additionally, NMCI and ONE-NET are constantly evolving and therefore the embarkation procedures are always changing, requiring tuning and automation when feasible, and identifying new procedures that must be performed to successfully integrate the Embarkables assets into IT-21.

Although the Embarkables processes for Marines and Airwings are implemented and are functional, capability gaps exist and impact the services provided to the end user and the security status of the workstation during deployment.

THIS PAGE INTENTIONALLY LEFT BLANK

III. EMBARKABLES ROOT CAUSE ANALYSYS

A. INTRODUCTION

From its conception in 2000 to its contract end in 2011, NMCI followed a contractor-owned contractor-operated (COCO) model for providing IT services to the Navy and Marine Corps. Alternatively, IT-21 and ONE-NET were under a government-owned government-operated (GOGO) model, in which the government owns and operates all network related activities. Although IT-21 and ONE-NET had a GOGO model, both networks were (and currently are) managed by different Program Offices and sourced through different funding lines.

The outcome of these programmatic differences and the uniqueness of environments the three networks operate under led to variations in design, capabilities, and operational and maintenance strategies across these networks.

As the DoD strives toward network alignment to maximize productivity and efficiency while minimizing cost, the immediate need for ashore units to embark into an IT-21 network with no downtime in productivity needs to be addressed in the short term. Embarkables mechanism and processes are in place to facilitate user mobility from network to network while maintaining adequate level of IT services in a timely manner, but these mechanisms have been designed and implemented as "quick fixes" to address the loss of IT services experienced by embarking units resulting from nonexistent interoperability between networks. Embarking units constantly face integration problems with IT-21 environments due to constant modifications on ashore and afloat environments and lack of Embarkables process standardization at the enterprise level.

Although the existing Embarkables mechanisms alleviate the immediate need to receive basic IT services during a deployment, they do not address the root cause of the network interoperability problem. This lack of interoperability adds labor intensive processes, induces risks due to manual intervention and adds costs to the Navy's mission.

This chapter identifies and analyzes the contributing factors and potential root causes affecting the Embarkables assets when connecting to an alternate network by

performing various analyses and implementing systems engineering tools. A Functional Decomposition was developed for a network as an ashore system providing common IT services (such as NMCI and ONE-NET). A traceability matrix maps system functions to customer needs previously identified in Table 1, followed by tracing those system functions to system components to identify those system components introducing technical and programmatic issues to the Embarkables integration into the afloat network.

A root cause analysis was performed by developing an Ishikawa cause and effect diagram, also known as a "fish bone" diagram, on the areas of most impact. The Ishikawa diagram identified contributing causes of the problem in five major categories leading to the identification of potential factors causing the overall effect. Identifying and understanding the relationships between these sources of variation is a key element to develop and implementing corrective courses of action.

B. FUNCTIONAL DECOMPOSITION AND TRACEABILITY

The Common Systems Function List (CSFL) v.9.1 by the Assistant Secretary of the Navy (ASN) Research, Development and Acquisition (RD&A) Chief Engineer provides the basis to identify functions for related C4I and net-centric system functions. The CSFL was utilized as the functional framework to develop a functional decomposition of a DoD network providing common IT services. The CSFL functional framework consists of five Tier 0 functions: 1.0-Combat, 2.0-Sustainment, 3.0-Business, 4.0-Enterprise Application Support Services and 5.0-Enterprise System Services.

Tier 0 functions 4.0-Enterprise Application Support Services and 5.0-Enterprise System Services cover most IT services provided by an ashore network. Additional functions such as 2.0-Sustainment and 3.5-Logistics also apply to the system but are not directly connected to the root cause of the Embarkables problem, therefore were not included in the functional decomposition. Figure 9 and Figure 10 illustrate Tier 0 and Tier 1 of the system functional decomposition for functions 4.0 and 5.0. Further decomposition was performed following the CSFL as guidelines down to Tier 5 where applicable and the list of system functions is provided in the Appendix.

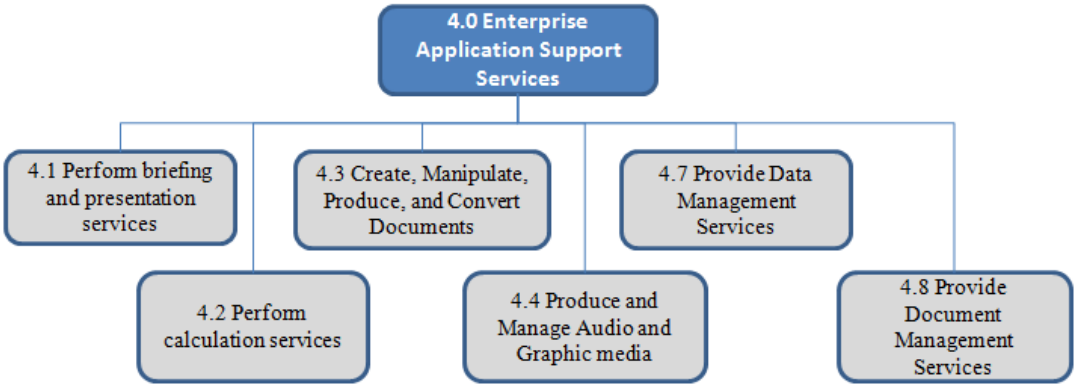

Figure 9. Enterprise Application Support Services Functional Decomposition

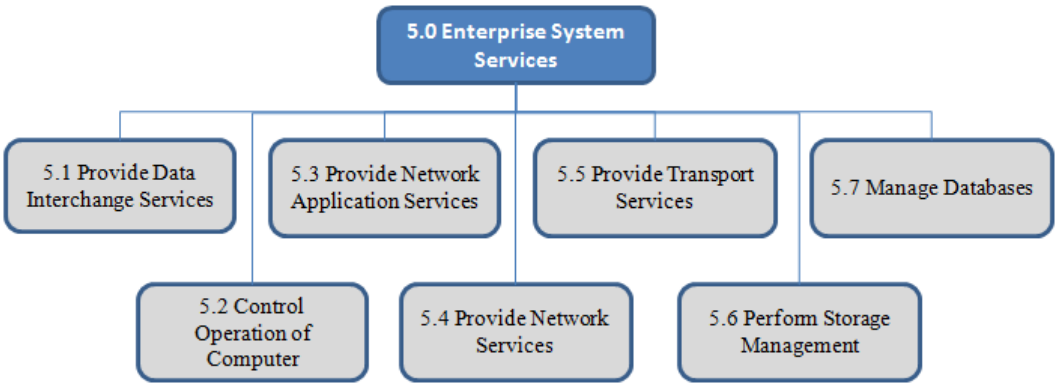

Figure 10. Enterprise System Services Functional Decomposition

System functions were mapped to User Case 2 needs (customer requirements) in a system function-to-customer requirements traceability matrix provided in Table 6. User Case 2 was the scenario used for the traceability matrix to represent single or small groups of embarking users without PPS and NAS devices. User needs colored in red represent unmet needs during an embarkation. Yellow fields represent those needs requiring additional reconfiguration to the network prior to Embarkables integration. Green fields represent the needs that seamlessly provided to User Case 2 by the host network.

NEED ID	USER NEEDS	SYSTEM FUNCTIONS
N1	Cryptographic logon to workstation (cached users)	4.2.8, 5.2
N2	Domain account	5.2, 5.4.4.1.8 - 5.4.4.1.13, 5.5
N3	Network access	5.2, 5.4.4.1.8 - 5.4.4.1.13, 5.3.5.5-5.3.5.6, 5.5.18-5.5.19
N4	Send/Receive Email	4.2.4.1, 4.8.1, 5.2, 5.3.5.5 - 5.3.5.6, 5.3.6.1 - 5.3.6.10, 5.4.4.1, 5.5.58, 5.5.15
N5	Attach and open email attachments	4.3.3, 4.8.3
N6	Access to Contacts	4.2.4.1, 5.2, 5.3.5, 5.3.6, 5.4.4.1, 5.4.5.1
N7	Access to Native Network Global Address List	4.2, 5.2, 5.3.6, 5.4.4.1, 5.4.5.1
N8	Ensure workstation protected from cyber attaches and spam	5.3.5.6, 5.4.4.1.9.7
N9	Shared Calendar	4.2.2.2, 5.4.4.1
N10	Accessibility to user data and email files on local hard disk such as .pst files as part of user profile	4.3.5, 4.7.2, 5.3.6.7 - 5.3.6.9
N11	Accessibility to user data and email files stored on the user home drive	4.3.5, 4.7.2, 5.3.6.7 - 5.3.6.9
N12	Outlook Capabilities (email settings, print styles, email rules and setting, etc)	4.2.2, 4.2.3, 4.2.4
N13	DOD digital email signature and encryption capability for home network email	4.2.14, 5.2, 5.4.4.1.9.7.1 - 5.4.4.1.9.7.3, 5.5.6, 5.5.19
N14	DOD digital email signature and encryption capability for host network email	4.2.14, 5.2, 5.4.4.1.9.7.1 - 5.4.4.1.9.7.3, 5.5.6, 5.5.19
N15	MS Office and Other local DoD approved apps for seat/user	4.1, 4.2.8, 4.3.1, 4.3.2, 4.3.3, 4.3.5, 4.4.5, 4.7.10, 4.8.3, 5.2, 5.7
N16	Protected data transmissions	5.4.4. - 5.4.5
N17	Web access and Cache	4.7.3, 5.3.5.6, 5.3.9, 5.4.4.1, 5.4.4.1.8
N18	Authentication Services—PKI/CAC	5.4.4.1.9.7.1, 5.5.19
N19	OS and application patching	5.4.4.1.9.7, 5.4.4.1.9.7.6
N20	Access to web based applications including certificate-based authentication applications	4.2.8, 4.7.3, 5.3.9, 5.5.19
N21	Native Home drive to view, edit, crate and delete files depending on use access	4.7.2, 4.7.10, 4.8.3, 5.3.5, 5.4.5.2, 5.5.18-5.5.19, 5.6.3
N22	Native Command shared drive to view, edit, crate and delete files depending on use access	4.8.3, 5.3.5, 5.5.18-5.5.19, 5.6.2, 5.6.3
N23	Access to Public Folders	4.7.2, 4.7.10, 4.8.3, 5.3.5, 5.4.4.1, 5.4.5.1, 5.5.18-5.5.19
N24	Local and network data integrity	4.7.11, 5.2, 5.3.5, 5.4.4.1.9.7.4, 5.6.1
N25	Locate and connect to home and share drives	5.2, 5.3.5, 5.4.4.1.8, 5.4.5, 5.5.18-5.5.19
N26	Seat Local Data storage capacity	4.7, 4.8.3, 5.2, 5.4.2
N27	Receive administrative policies and user privileges	5.4.4.1, 5.5.18
N28	Security policies applied to account	5.4.4.1.9.7, 5.5.18
N29	Application management	5.3.0
N30	Air Card and Wireless capability	5.4.4.1.6, 5.4.5.6
N31	Print/Scan/Fax capabilities	4.4.2, 5.4.4.1.8, 5.4.5.3, 5.5.9, 5.5.15
N32	Locate and connect to printers	5.2, 5.4.5.3, 5.5
N33	Chat and Instant Messaging (IM)	4.2.10, 4.2.11, 5.2, 5.4.5.4
N34	Access to collaboration tools (i.e. Defense Connect Online (DCO)	4.2.12, 5.3.5, 5.5
N35	Command Document collaboration / Portal (SharePoint)	4.7, 4.8.3, 5.1, 5.3.5, 5.5.18,5.5.19
N36	24/7 Help Desk	3.5.2.1-3.5.2.2,
N37	Technical support	3.5.2.1-3.5.2.2, 5.4.4.1.9.8
N38	Capability to create a trouble ticket and check status	3.5.2.1-3.5.2.2
N39	Training capabilities	3.5.2.3.8
N40	Tech Refresh	3.4.1
N41	HW repair or spares (PUK)	3.5.2
N42	Capability to transfer files	5.2, 5.3.5, 5.4.5.3, 5.5
N43	Messaging—Alerts	4.2.11, 5.4.5, 5.5
N44	Secure, available and reliable network connection (99% Service Level Agreement)	5.3.1-5.3.3, 5.5
N45	Backup and Restore Capability	5.3.1-5.3.3, 5.6.1-5.6.2
N46	MAC (Move, Add, Change) Capability	5.3.1-5.3.4, 5.7
N47	VTC capabilities	4.2.13, 5.5
N48	Access to IT-21 Global Address List	5.2, 5.3.6, 5.4.5.1
N49	Access to IT-21 resources such as applications	4.2.8, 4.7.3, 5.3.9, 5.5.19
N50	Ability to store to external media	4.2.15, 4.4.7, 4.8.3, 5.3.1-5.3.3
N51	Produce and Manage Audio and Graphic Media	4.4.3
N52	Disconnect/Log out	5.2, 5.5.9, 5.5.15
N53	Ensure non repudiation	5.4.4.1.9.7.3
N54	Receive all Computer Network Defense policies and mandates (HBSS/DAR/etc)	5.4.4.1.9.7, 5.4.4.1.9.7.6

Seamless or provided by PPS and NAS
Provided by the IT-21 environment
Not available

Table 6. Need-to-Function Mapping

Analyzing the system requirement gaps (in red and yellow) and their respective system functions, the most reoccurring functions and those impacting high-priority IT services such as e-mail are identified in Table 7. These system functions were mapped to system components to identify those components causing or contributing to the deficiency of network services provided to embarking units.

FUNCTION	Back End Architecture	Network Management system	IA	PC image
4.2 Perform Calculation Services				
4.2.2.2 Shared Calendaring	X			
4.2.8 Manage Desktop Communication Applications	X		X	X
4.7 Data Management Services				
4.7.2 Conduct Data Storage/Retrieval/Updating	X			
5.3 Provide Network Applications Services				
5.3.0 System functions that provide the capability to access and use applications on the network				X
5.3.5 Disseminate operational/tactical information		X		
5.3.6 Exchange electronic mail	X			
5.3.8 Provide network applications scalability				X
5.4 Provide Network Services				
5.4.4.1.9 Manage network operations		X		
5.4.4.1.9.3 Perform account management	X			
5.4.4.1.9.7 Perform network information assurance/security management		X	X	
5.4.5 Provide Networking Desktop Services				
5.4.5.1 Provide Directory Services	X			
5.4.5.2 Share Files and Printers	X			
5.5 Provide Transport Services				
5.5.17 Access Control	X		X	
5.5.18 Role / Privilege Management	X			
5.5.19 User Management	X			

Table 7. Function to Component Mapping

The Back-End-Architecture system form is the component which introduces the most IT service deficiencies for an embarking system. Network management, IA and Workstation image also contribute to the system interoperability between networks as illustrated in Table 7**.**

The system components were further analyzed to identify root causes resulting network interoperability: (1) Network management including IA, (2) Back-End-Architecture, and (3) PC image.

C. ENTERPRISE NETWORK MANAGEMENT

As new computer network technologies constantly emerge and mature, DoD leverages and further enhances these technologies for communication capabilities with the goal of information superiority around the globe. Consequently, networks are increasing in size, capabilities, and complexity, requiring active managing and monitoring of all network assets to promptly and efficiently diagnose any problems, mitigate any possible risk, prevent and remediate network vulnerabilities, identify possible security threats, and secure the networks' integrity, confidentiality and availability.

Adversaries aggressively seek to penetrate and damage DoD networks with cyber-attacks and continuous malicious activities which threaten tactical information and overall DoD missions. Securing DoD networks is essential to attain and maintain data's integrity, information sharing, situational awareness and mission effectiveness. Directives and regulations for the monitoring, detecting, reporting and remediating of any network vulnerabilities or threats to computer networks are enforced at every level of the Computer Network Defense (CND) structure as illustrated in Figure 11. Security policies must be implemented at every layer of the CND. All these layers, from the desktop level to the DoD Global Integration Grid, are constant targets of physical and cyber attacks and require the implementation of security mandates to secure the network at every level such as: IAVA compliance at the desktop, LAN and WAN layers; HBSS at the desktop and DON GIG, Data at rest at the desktop level; and IP Blocking at the LAN, WAN and GIG layers to name a few.

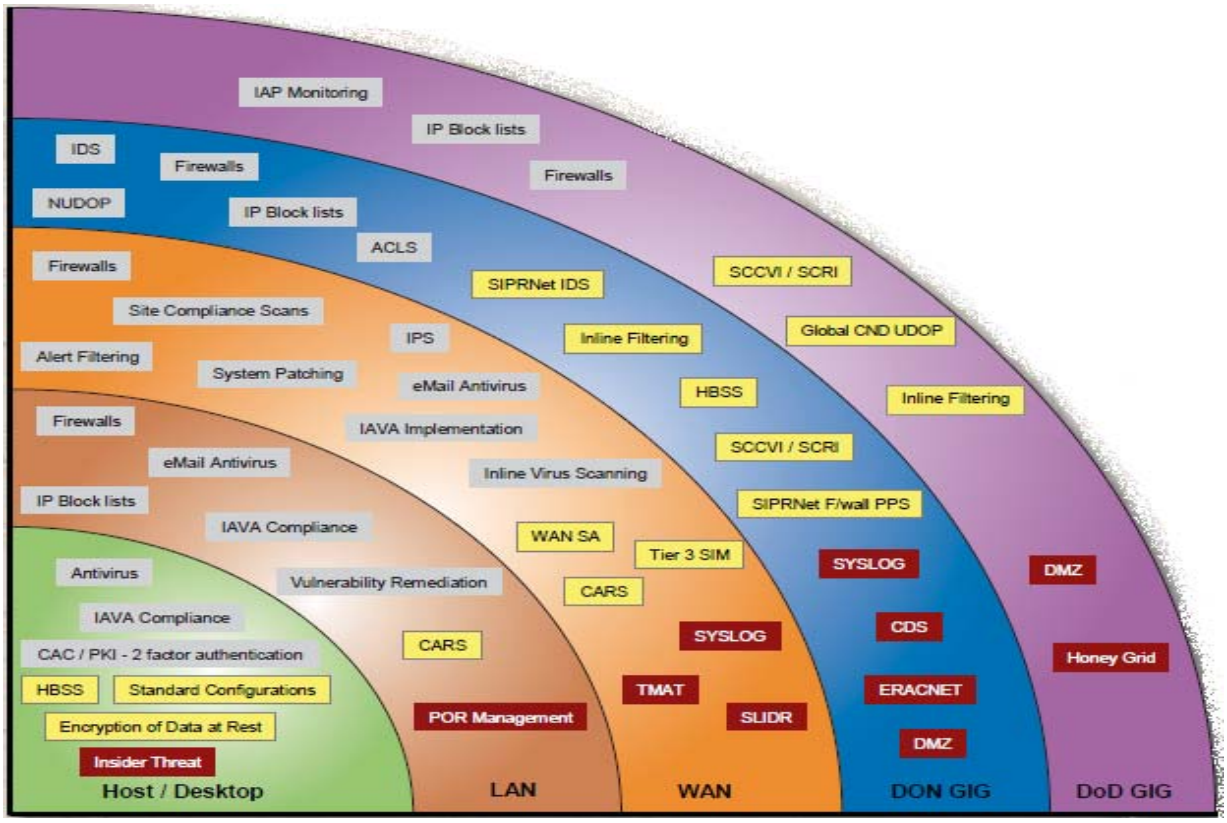

Figure 11. Computer Network Defense (From Department of the Navy Chief Information Officer, 2009)

Managing, securing and maintaining Navy networks requires advanced enterprise management solutions consisting of physical structure, tools, policies and processes strictly enforced. Network management solutions comprise software and hardware components as well as processes operating cohesively to secure the network by performing a variety of functions: server and application monitoring, operating system and application patching, security posture enforcement and screening, software distribution, change management, trouble ticketing, asset management and inventory collection of hardware and software.

IT-21, NMCI and ONE-NET developed customized network management solutions based on their unique needs and operational constraints. ONE-NET Enterprise Management System (EMS) core is an International Business Machines (IBM) Tivoli framework product which uses one single agent active at the network hosts to provide all

EMS functionalities (Purhagan, 2010). IT-21 uses Microsoft Systems Center Configuration Manager (SCCM) for patch management, software distribution and inventory. IT-21 is currently deploying an enterprise patch management solution for all PMW-160 POR system utilizing a Microsoft Windows Server Update Services (WSUS). NMCI uses Radia for patch management and software distribution; NetMeeting is used for remote control access as NMCI help desk is contractually obligated to obtain user permission to remotely access the workstation during an incident ticket resolution process. NMCI recently migrated from BCM Remedy to Service Manager (SM) 7.0 for Incident ticket creation and monitoring, including self service ticketing.

Table 8 summarizes the functionalities provided by the enterprise management systems and the tools utilized by each network.

Functionality	IT-21	NMCI	ONE-NET
Patch Management	SCCM 2007	Radia	IBM Tivoli Configuration Manager (TCM)
Software Distribution	SCCM 2007	Radia	IBM Tivoli (TCM)
Remote Control	SCCM 2007	NetMeeting Remote Desktop Connect	IBM Tivoli Remote Control (RC)
Incident Ticketing	BCM Remedy	SM 7.0	BCM Remedy
Inventory	SCCM 2007	Radia	IBM Tivoli (TCM)
Monitoring	SCCM 2007	Data not available	IBM Tivoli Monitoring
Network monitoring	WhatsUpGold 2.5	Cisco Works	IBM Tivoli NetView
Event Management	SCCM 2007	Data not available	IBM Tivoli Enterprise Console (TEC)
Image Deployment	SCCM 2007	SM 7.0	IBM Tivoli (TCM)
Computer Defense Network	McAfee's Hercules 4.5	Radia	IBM Tivoli

Table 8. Network Management Functions and Tools (After Podwoski, 2011; Navy Marine Corps Intranet, 2009; and Purhagan, 2010)

Securing Navy networks has become the primary function for the network management system by enforcing Information Assurance (IA) DoD directives to maintain compliance on the security posture across the enterprise. The DoD Directive (DODD) 8500.01E and the Chairman of the Joint Chief of Staff Instruction 6510.01F provide direction and guidance on the implementation of security requirements, controls,

protection mechanisms and standards for all DoD owned or controlled information systems that receive, process, store, display or transmit DoD information, regardless of mission assurance category, classification or sensitivity (Department of Defense, 2007). This is accomplished via an effective network management tool and process as part of the enterprise network management solution.

Navy and Marine workstations stay compliant while connected to their home network by constantly receiving security updates and OS and application patches. Embarked workstations connecting to an alternate network experience loss of connectivity to their native network disabling the ability to be centrally managed, thereby impacting the functionally of the following key subsystems to maintain the IA compliance: Data at Rest (DAR), HBSS, Network Access Control, Secure Configuration Compliance Validation Initiative/Secure Configuration Remediation Initiative (SCCVI/SCRI), Digital signature matching, Cryptographic Log-On (CLO) Authentication, User Based Enforcement (UBE), Firewall, GPOs, and Cached Login Credentials.

The following subsections identify network interoperability deficiencies for a seamless integration of Embarkables workstations into the afloat network affecting patch management; DAR; and HBSS policy enforcement, monitoring and reporting.

1. Patch Management

Operating system and application software vulnerabilities of one or multiple assets introduce security risks to the entire network to which the assets are connected. To correct such vulnerabilities, software fixes called ‘patches’ are pushed to the network when vulnerabilities are identified. Patch management is a key method to enforce network security by identifying, monitoring, mitigating and remediating software vulnerabilities. Timely identification of un-patched software and a prompt and effective enterprise remediation action is essential to secure Navy networks and their data.

This subsection identifies potential factors causing the patching deficiencies by developing an Ishikawa diagram to determine any technical and programmatic elements resulting in the inability for ashore workstations to seamlessly receive software patches

from the IT-21 network during a deployment. These potential factors were identified by reviewing IT-21, NMCI and ONE-NET documentation and interviewing subject matter experts on the following:

- The patch distribution and management processes for the IT-21 network and the Embarkables patching process to identify gaps in these methods and the driving factors for those variations.
- The network management tools utilized to perform all patching and software distribution functions by each network to identify discontinuity in meeting network patching requirements and tool incompatibility, resulting in the inability to leverage the IT-21 network management tools while connected to its topology.
- The operational environment each network operates under and how elements related to the environment were decision drives for the tool selection and the employed patching process.
- The operating commands and personnel managing these tools and processes to determine procedures' ownership, and manpower limitations such as lack of cross-trained personnel to identify how personnel affect the overall patching of Embarkables.

The contributing causes for these factors were grouped under four major categories: Equipment, Environment, Processes and People in the Ishikawa diagram. Potential contributing components for each category were identified by implementing the 5 Why's technique where appropriate to further identify root causes and any relationships between these causes directly or indirectly impacting the overall effect: the inability for Embarkables to receive patches when connected to the IT-21 ISNS LAN.

a. Network Management Tools

Software patch distribution and management requires a customized patching process and deployment tool to release patches and hot-fixes across to the enterprise. Network management and patching tool features include: manipulating

security configuration settings, deploying standard software packages, scanning OS and applications, monitoring and reporting, and maintaining policy compliance by taking an active role in vulnerability remediation. IT-21, NMCI and ONE-NET have fielded customized network management processes and use different management tools to scan and patch their client and server infrastructures.

IT-21: IT-21 supports COMPOSE versions 2.x to 4.x on shipboard ISNS LANs and the patching process varies based on the COMPOSE baseline. Most ships are on COMPOSE v3.0 or higher versions and use SCCM, a Microsoft product for managing windows based computer systems and provides remote client and server control, patch and software management, and operating system deployment (Program Manager Warfare 160, 2011). First introduced with COMPOSE v3.0, the SCCM product did not support a Tiered environment (such as NMCI and ONE-NET) but this was not a requirement for IT-21.

NMCI: The new HP Client Automation Enterprise (CAE) system (using Radia at the client) is used as the software and patch manager for NMCI assets. CAE automates scheduled night connections to deliver software and Radia Daily Connect for startup and login scripts at boot up.

ONE-NET: ONE-NET's Enterprise Management System uses the IBM Tivoli line of products including the IBM Tivoli Configuration Manager for patch and software distribution. It uses Windows Patch Management System (WPMS) to push OS, application patches and software to maintain the Information Assurance Vulnerability Management (IAVM) compliance (Purhagan, 2010).

Table 9 summarizes the different tools used for patch management and software distribution by the three networks resulting in tool incompatibility across network environments.

Network	Network management tool	Vendor
IT-21	SCCM	Microsoft
NMCI	Radia	Hewlett-Packard
ONE-NET	Tivoli	IBM

Table 9. Network Management Tools (After Purhagan, 2010 and (Program Manager Warfare 160, 2011)

b. Patching Process

Each network has an effective patch management process for its workstations to receive all required patches while connected to their native network to maintain compliance and for delivering software to the enterprise.

IT-21: Deployed ships are unable to use terrestrial-based systems for communications and the only method of communication to ashore facilities is via satellite links. This limitation introduces a challenge to patch management for IT-21 and Embarkables assets due to the limited bandwidth available during deployment as monthly and critical patch pulls result in high bandwidth requirements on the already saturated SATCOM links.

DISA manages a notification service which provides information on trusted and authenticated Microsoft and other software patches to be disseminated to DoD networks. IT-21 identifies applicable patches to each COMPOSE environment and makes those accessible at the POR approved patch repositories: the Naval Networks and Sailor websites.

Shipboard administrators manually initiate the download from the patch repositories and determine which patches apply to their platform configuration. Due to the size of some of these patches, ship to shore synchronization and pull of patches are scheduled during non-critical fleet operations. Patch pulls often congest the SATCOM links and fail due to size of patch and the latency of the connection. After patches have been downloaded and are available on the ship's LAN, pushing patches to all the assets must be carefully planned and security considerations addressed. The security patch

deployment instructions recommend scaling down the number of simultaneous workstations installations to prevent any degradation of network performance due to the heavy traffic load.

IT-21 patching process using the WSUS incorporates a 3rd party tool called EminentWare to patch non-Microsoft Windows-based applications on all COMPOSE 3.x or higher environments and other applicable PMW-160 systems including coalition networks as CENTRIXS-M. Together, these tools automate the delivery and implementation of software patches to the fleet, providing more control as to when patches are pulled to ensure no impact on ship's operations (Program Manager Warfare 160, 2011).

WSUS provides a hands-off approach to downloading and managing software updates. The service automatically synchronizes with upstream WSUS servers to remain up to date with the most recently approved updates for Microsoft applications as well as Windows-based non-Microsoft applications that have been configured to communicate with WSUS. Once synchronization is complete, WSUS manages installations for all updates and provides reporting capability for Microsoft updates (Department of the Navy PMW160, 2011). Non-Microsoft patches are managed and reported through InfoPath forms. Information on new updates and update approvals are delivered to downstream servers, and update installation and client requirements data is transmitted to the upstream server during scheduled synchronizations. Any updates are created on the master servers and replicate throughout the organization in a downstream fashion: software support activities' master servers to the NOCs to the ships.

While IT-21 is standardizing the patch management solution across the IT-21 environment using the WSUS, this new patching solution has not been tested for Embarkables workstations. The use of the WSUS would eliminate the need for the Unit IT to initiate the patching process by downloading appropriate patches from the NMCI Home port website or Naval Networks websites. Patching Embarkables seats remains an isolated process to the ship's patch management process.

NMCI Embarkables process: NMCI patches are packaged, tested and posted on the websites for download. For large deployers, the Unit IT is responsible to download patches to a source patch directory to be accessible to all workstations and servers requiring patching. For small groups or single users without Unit IT, it is the user and the ship's responsibly to maintain compliance. NMCI developed the Deployables Unmanaged Patch (U-Patch) Utility solution to aid the deployed units validate and update their Client Data Seat's IAV security posture, and to distribute patches and security updates to NMCI embarked assets.

The U-Patch Utility is part of the deployable workstation baseline. A server or workstation is assigned as the patch repository to keep all required network patches for the embarking units. During deployment, the source directory for patches must be configured on all workstations and it must be accessible to the logged user with the proper read permissions. U-Patch utility runs in silent mode on each asset, each time a user logs on the utility checks for new patches to download and process. The frequency the seat checks for new patches can also be configured. Critical patches can be forced to run after the user has logged on to the seat. For workstations without U-Patch or without access to the source directory, manual patching must be performed by the user or IT staff to maintain compliance.

ONE-NET Embarkables process: It is the Unit IT's and ship staff's responsibility to maintain all seats and PPS servers IAVA compliant by delivering applicable ONE-NET patches which are available for download from the PMW-160 Naval Network Web-page. ONE-NET facilitates seat patching with the implementation of the Deployable Workstation Management (DWM) Patch Distro tool. The DWM tool performs discovery of ONE-NET workstations in the Embarkables or ship domain requiring patching, and an executable file (dwm.exe) performs the patching (Purhagan, 2010).

c. Operating Environment

During a deployment or when terrestrial connectivity is unavailable, Navy vessels depend on military satellite communication systems augmented by commercial

satellite systems to enhance the capability, reliably and performance of radio frequency connectivity back to shore. This operational environment introduces bandwidth constraints and connection latency issues furthered discussed Section D. The unique circumstances the ships encounter during deployment influence the afloat patching process. The intermittent SATCOM connection to the shore limits the software patch download and the internal patch distribution to its assets. Most patches are large in size and the link's latency and intermittent connection result in patch download failures. Additional environment limitations and their impact on the Embarkables patching deficiency is illustrated in Figure 12.

d. People

Although the three networks are owned by NETWARCOM, they are managed by different program offices and sourced through different funding lines. PMW 205 manages NMCI and ONE-NET while PMW 160 manages the IT-21 network. During deployment, it is the Embarkables Unit IT's responsibility to ensure that the hundreds of embarking assets (servers and workstations) are properly patched throughout the duration of the deployment. This is a time consuming task to perform, it must be manually initiated and any workstation not properly receiving patches must be physically visited by the Unit IT.

The ship's staff is unavailable to support the Embarkables patching process as their primary responsibility is to support the ship's users and communications. Additionally, the ship's staff uses a different patching process and patching tool compared to the Embarkables tool; this unfamiliarity contributes to the limited support they can provide to the patching of Embarkables assets.

The identified causes for each category were grouped under their respective categories to construct the Ishikawa diagram depicted in Figure 12.

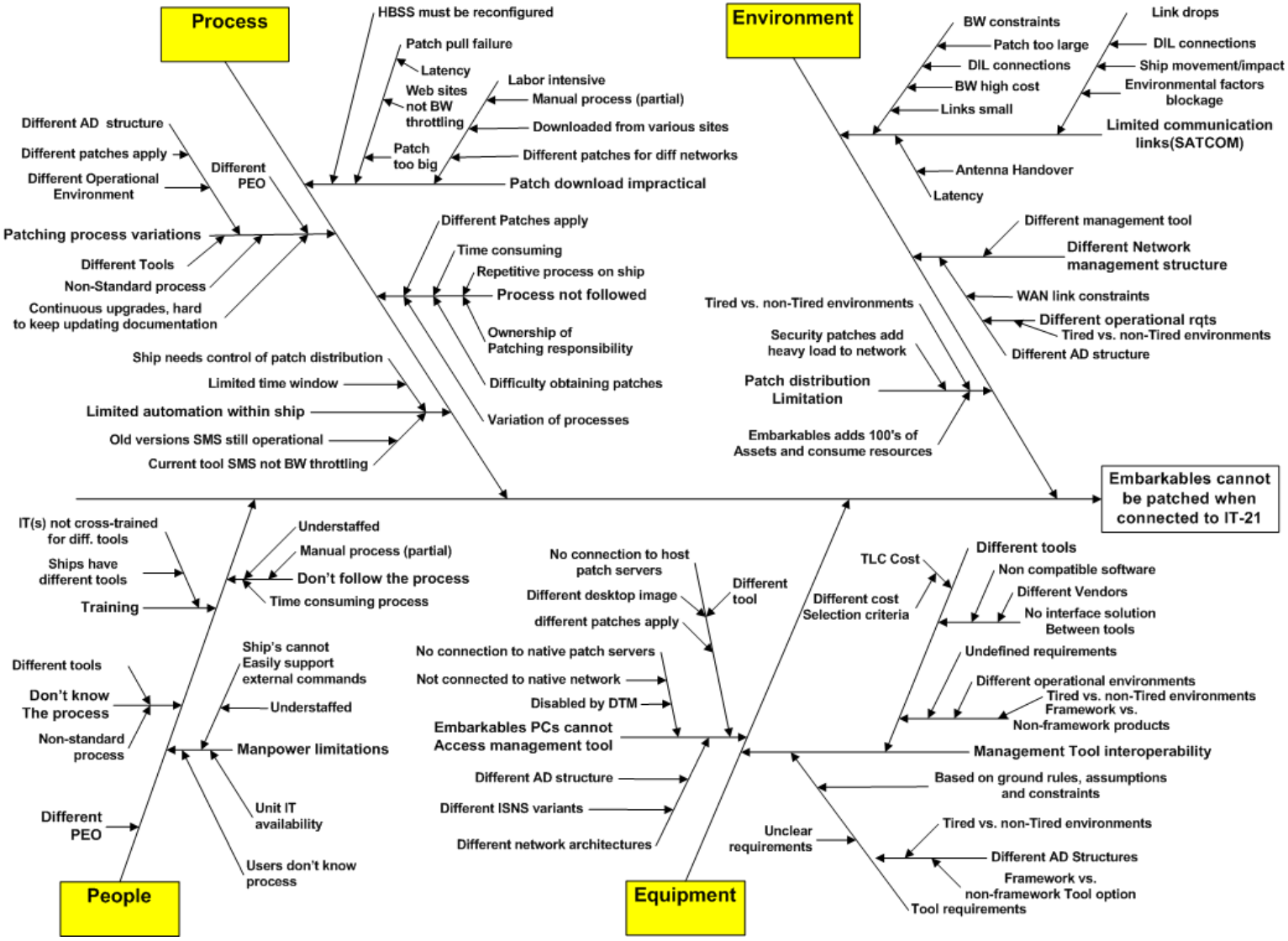

Figure 12. Ishikawa Diagram for Patch Management

As illustrated in the Ishikawa diagram, the environment category introduces the operational environment variation impacting the Embarkables ability to receive patches during deployment. This category identified possible factors resulting in the inability to receive Embarkables patches during deployment, such as the large size of the patches, the bandwidth limitation and intermittent SATCOM links. It also identified the contributing factors impeding the utilization of shipboard patching tools, such as the difference in tools currently used to patch the network assets, and the interoperability between these tools.

The Process category identifies the variations in patching processes implemented by the IT-21 network and the ashore networks, the impractical and inconsistent process to download applicable patches for Embarkables seats, how the difference in management tools drive variations in patching process, and the fact that different networks require different patches to be applied to their assets.

Under the People category, the variation in process and the different patching tools contribute to the inability to leverage the ship's IT personnel to patch Embarkables seats during deployment as they are unfamiliar with the ashore process and tools.

The Equipment category identifies the difference in patching tools and possible root causes of that variation, including cost factor and the network requirements driving the selection of different tools by each program office to be implemented on their network.

To summarize, the following sub-causes have the most influence on the four major categories: (1) Differences in patch management tools: Embarkables units cannot be centrally managed by the IT-21 network due to different management tools used which are not compatible, resulting in the need for an Embarkables utility; (2) The patching process requires a manual download of afloat patches during deployment and is one of the causes of the inability to patch seats: the size of patches is too big to download via SATCOM; low bandwidth, high latency and intermittent connection causes patch downloads to fail; Unit IT must manually search for patches that apply to the Embarkables seats which is time consuming and could result in the wrong patch

attempting to be applied; (3) Different patches apply: IT-21 image and applications require different patches than the NMCI and ONE-NET images.

The different AD structures derive from the different environments the three networks operate under. Management tool interoperability is due to the difference in tools utilized which were selected based on requirements, cost, and constraints. Furthermore, unclear requirements contributed to the difference in tool selection as each network worked independently on the patch management process around its constraints and to meet is specific operational needs.

2. Advanced Client Security Policies – Data at Rest (DAR)

Malicious or non-malicious network vulnerabilities that are introduced into the network contribute to the constant loss of sensitive information, placing the armed forces at risk. Some of these vulnerabilities result from negligence or failure to protect both data in transit and data at rest on DON networks. On July 3, 2007, the DoD Chief Information Officer (CIO) issued a memorandum establishing a DoD policy to protect sensitive unclassified information on mobile computing devices and removable media (Space and Naval Warfare Systems Center, 2010).

DAR refers to all data stored on hard drives, thumb drives, Compact Discs/Digital Versatile Discs (CD/DVD), floppy diskettes, and similar storage media. It excludes data that is traversing a network or temporarily residing in computer memory to be read or updated (Metz, 2006). DAR is composed of several integrated elements to provide a complete data protection platform to the enterprise: (1) Hard Disk Encryption, (2) Removable Storage Encryption (RSE), and (3) Advanced Authentication Pre-Boot Authentication (PBA).

- Hard Disk Encryption protects against unauthorized reading or copying of data off a protected hard drive. It encrypts a workstation's hard drive when it is powered off and auto-decrypts it when the workstation boots up.
- RSE encrypts data copied to a removable storage device, CD/DVD, it protects all data transferred off a DAR-protected workstations and it is operable with non-DAR workstations.

- PBA allows registered users to boot workstations following user authentication using a common access card (CAC) or alternative logon token. Only registered CAC certificates loaded in workstation memory would be authorized.

DAR uses the user's Public Key Infrastructure (PKI) encryption certificate within the DoD CAC to protect the full volume encryption key. Multiple users on the workstation or device are able to use their individual DoD smart cards for boot authentication. Figure 13 illustrates the DAR concept.

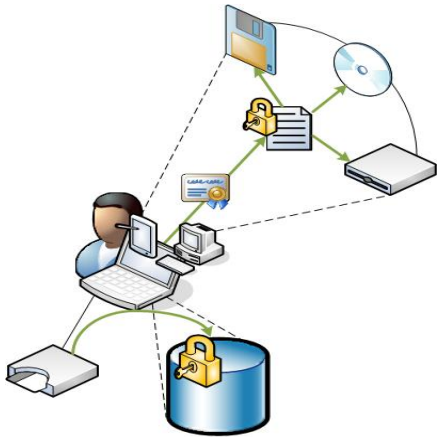

Figure 13. DAR for Hard Disk and Removable Storage (From Space and Naval Warfare Systems Center, 2009)

a. DAR Solutions for DON Networks

DoD approved eleven DAR solutions, including Mobile Armor and GuardianEdge (GE) encryption solutions. GE was selected for NMCI and ONE-NET, and Mobile Armor for the other Navy networks. Networks require waivers to employ a different encryption solution by other than GE and Mobile Armor. DON selection of alternatives was influenced by the Embarkables requirements to administer workstation during deployments. Selecting a different DAR encryption solution for ashore and afloat networks allows for local administrators to have certain privileges to continue managing workstations when connecting to IT-21 during deployments.

Table 10 summarizes the DAR solutions (or future implementation) by each network.

Network	Encryption Software	Version	Vendor
IT-21	Mobile Armor (future)	n/a	Mobile Armor (future)
NMCI	GuardianEdge Products	9.5.x	Symantec (formerly GE)
ONE-NET	GuardianEdge Products	9.1.5	Symantec (formerly GE)

Table 10. DAR Software Solution Summary Table

NMCI has deployed all three elements of DAR using GE Encryption Anywhere (GE EA) software, and the GE Removable Storage (GERS) utility. It is also enforcing PBA where a workstation boots after cached user has been authenticated.

ONE-NET's GE EA Platform is based on a modular design that contains three functional components: GE Data Protection Framework, the GE Manager (DAR Manager) and the Client modules GE Hard Disk Encryption, GERS and GE EA. The implemented ONE-NET DAR solution includes the Hard Disk Encryption and the Removable Storage Encryption elements; PBA has not been deployed on ONE-NET.

IT-21 DAR solution is under development and has not fielded any data at rest encryption capabilities to date.

b. DAR and Embarkables

DoD Directive on protecting data at rest applies to all DON systems regardless of the network they are connecting to or their deployment status. NMCI and ONE-NET assets deploying into IT-21 must comply with the CIO directive by employing DAR even during deployment state.

NMCI and ONE-NET DAR solutions consisting of GE products continue working in a disconnected or deployed state. Workstations however, do require regular connectivity to DAR servers for GPO updates, recovery key check-in (for back-up recovery functions), status information stored on server, and to rebuild a workstation whose hard drive is inaccessible. This connection back to the DAR services is unavailable for workstations connecting to the afloat network.

Workstations' hard disks are encrypted (with the exception of the bootstrap files necessary to boot the system) by GE when a workstation is shut down and

its data is protected while residing on the hard drive. Data is then auto-decrypted by GE products at boot up and accessible to the user. A GE Hard Disk encryption feature is to lock a protected workstation that has failed to check with the DAR Manager (located at the shore) within a specified number of days. If this feature is implemented, the hard disk would be locked and would require a client administrator to unlock. This feature is currently not implemented by any network.

DAR Embarkables users can encrypt files on removable storage devices and those files can be decrypted by IT-21 or any other workstation with different DAR solution or with no DAR solution at all. This is accomplished by copying the GE Technologies Access Utility into the removable storage devices, to be used by decrypting workstations. This allows data mobility during a deployment.

While DAR solution works in isolation, it enforces stringent local security workstation policies which hamper the Embarkables process. Embarkables require escalated privileges to workstations for the Unit IT to reconfigure the network management agents, network configuration, data migration functions, reimage and rebuild seats, unlock GE Hard Disk-protected workstations and unregister GE users. This ability to administer a seat cannot be locked by DAR or be lowered down to a user access in order for the Embarking Unit IT to be able to successfully connect into the IT-21 LAN.

To mitigate this issue, Unit IT(s) are provided with client administrator password to enable them to perform the administrative functions required during deployment. Preset Client Administrators are allowed to access the workstation by authenticating (using a username and password) to GEHD at the logon prompt and to Windows at the Windows logon prompt and are not required to authenticate with a DoD CAC. These accounts are inserted into the client software installation package prior to deployment and cannot be modified during a deployment. These accounts ensure the Unit IT can unregister GE users and decrypt a partition or partitions regardless of GPO processing (Space and Naval Warfare Systems Center, 2009).

When System restore tools are used to repair a corrupt boot section on the workstation’s hard drive, a common tool is the IBM Rescue and Recover application.

This application requires the Master Boot Record (MBR) to be properly configured for the application to function and it replaces it with its own settings. GEHD relies on the MBR and modifying it results in system problems. GEHD incompatibly with some system restore tools which modify the MDR results in unbootable systems making it very difficult to retrieve the data on the hard disk.

Although the status quo permits encrypted data mobility between networks, workstations cannot be centrally managed; there is no reporting to the DAR manager; there is no implementation of GPO updates; and Unit IT(s) require a client administrator account and procedure to integrate the workstation into the network and to unsure functionally.

Current afloat DAR solutions, although using the same products, are not compatible with each other or with other networks. To perform integration with other networks, an alternate product or GuardianEdge 9.3 or higher is required in both environments. NMCI is currently on 9.5.x and ONE-Net on 9.1.5 (Space and Naval Warfare Systems Center, 2009).

3. Host Based Security System HBSS

On October 9, 2007, the Joint Task Force for Global Network Operations (JTF-GNO) released Communications Tasking Order (CTO) 07–12 mandating the deployment of the Host Based Security System (HBSS) on all combatant command, service and agency secure and non-secure networks within DoD (LandWarNet, 2008).

The HBSS baseline is a COTS-based application for the detection, monitoring, and countering against known cyber-threats to DoD Enterprise. It is attached to each host (server, desktop, and laptop) in DoD, managed by local administrators and configured to address known exploit traffic using an Intrusion Prevention System (IPS) and host firewall. DISA provides guidance regarding the deployment and operations of HBSS, defines baselines and configuration settings consistent with DoD requirements and guidance, and revises/concurs with all deviations from HBSS architecture necessary for operational requirements. DISA provides HBSS software (i.e. patches and hot fixes) available for download to the DoD community (Defense Information Systems Agency,

2010). Each DoD network is responsible for developing an HBSS solution to meet all DISA mandates and adhere to policies, define network specific configurations, and test solutions and updates prior to deployment.

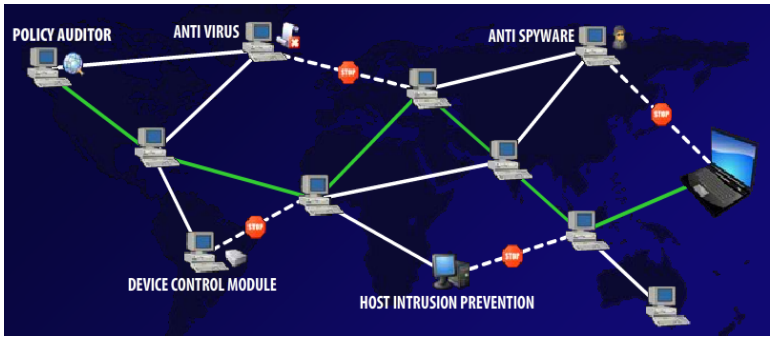

Figure 14. HBSS concept (From Defense Information Systems Agency, 2011)

HBSS is currently at baseline v4.5, Maintenance Release 2.0 (MR2). It is composed of multiple software applications, which together provide system management, policy enforcement and reporting capabilities consisting of the following McAfee products (Defense Information Systems Agency, 2010):

- ePolicy Orchestrator (ePO) server– responsible for collecting and displaying events, controlling policies, and managing the product modules at the clients via the McAfee agent.
- Host Intrusion Prevention System (HIPS) - protect against known and unknown malicious activity including, worms, Trojan horses, buffer overflow attacks, malformed commands, critical system file modifications, unauthorized access to system resources and privilege escalation.
- Policy Auditor (PA) is responsible for ensuring compliance with information security mandates such as Federal Information Security Management Act of 2002 (FISMA).
- The Assets Baseline Module - addresses system baseline configurations and changes to respond to Information Operations Condition (INFOCON) changes necessary during times of heightened security threats to the system.
- The Rogue System Detector (RSD) - provides real-time detection of new hosts attaching to the network.
- Device Control Module/Data Loss Prevention - The DCM component address the use of USB devices on DoD Networks.

The HBSS McAfee Agent (HBSSMA) on clients provides the basic communication mechanism between workstations and ePO server. It is used by the ePO server to enforce policies, reporting, product deployment, detection of possible rogue systems connecting to the network, and management of all HBSS modules at the clients. The HBSS architecture overview is depicted in Figure 15.

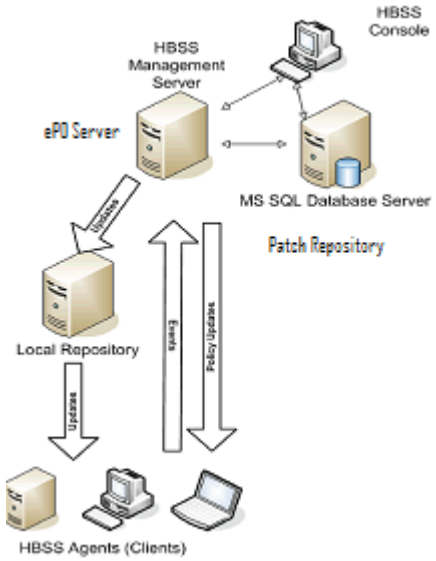

Figure 15. HBSS Architecture Overview (From Defense Information Systems Agency, 2009)

c. HBSS solution on DON networks

IT-21, NMCI and ONE-NET have deployed DISA's HBSS architecture and polices, and constantly update HBSS baseline versions to ensure compliance with CTO 07–12. IT-21 is currently deploying HBSS 3.0. NMCI has upgraded to baseline HBSS 4.5 MR2 while ONE-NET is currently deploying the same version at TNOSCs.

Network	HBSS	Vendor
IT-21	HBSS 3.0 (deploying)	McAfee
NMCI	HBSS 4.5 MR2	McAfee
ONE-NET	HBSS 4.5 MR2	McAfee

Table 11. HBSS Baselines on Navy networks

Table 11 summarizes the current HBSS baselines on the three DON networks. At present, there are different HBSS baselines fielded at the operational environment resulting in a miss-match of agents on clients and servers when connecting across networks. DISA has released an expiration notification for HBSS 3.0 by February 29, 2012 to all entities to upgrade to current HBSS baseline 4.5 MR2 in order to continue obtaining maintenance support. Such mandates force navy networks to deploy the latest versions and achieve baseline consistency across networks, but some networks are falling behind with the upgrades.

d. HBSS on Embarkables

NMCI and ONE-NET HBSS suite encounters interoperability issues while attempting to connect to IT-21 HBSS suite during an embarkation event. This interoperability goes beyond the version difference between the networks. This subsection explores and identifies the HBSS components and configuration inconsistencies causing Embarkables' problems.

HBSSMA connection to ePO server: Embarkables workstations loaded with McAfee agent v4.5 and v4.0 are unable to communicate with the ship's ePO server currently running on HBSS v3.0 due to: (1) ePO directory paths on workstations point to the ePO server of native network, therefore it would fail to establish a required secure communication with ship's ePO server; (2) a mismatch of certification key pair and ports used to encrypt/decrypt communication traffic between the ePO server and clients (HBSS v3.0 communicates via port 80, HBSS v4.5 communicates via port 443); (3) a mismatch of IP addresses and ports configuration on the B2 firewall when a embarked client attempts to connect to its native ePO server; (4) mismatch of IP addresses and ports configuration on the ePO server's firewall (Hoang, 2011).

Host Intrusion Prevention System problems: HIPS uses the ePO framework for delivering and enforcing HBSS policies at the enterprise. One of HIPS features is the host based firewall which acts as a filter between the workstation and the network to which it is connected. The host firewall is configured with policies for inbound and outbound traffic for network resources such as exchange, web server, and

domain controller. It also defines the type of traffic allowed, applications, IP addresses and address ranges specific to the native network. During a deployment, the embarking workstation's firewall is configured to allow traffic from its native network's information such as application ports, protocols, and IP addresses. When connecting to the IT-21 environment, the firewall might not identify IT-21 network information and block traffic between the workstation and the network servers.

HIPS policies affect Embarkables printing capabilities. Limited physical infrastructure and LAN drops onboard ships generate the need to share printers directly connected to a workstation. NMCI and ONE-NET HIPS policies do not allow the sharing of non-networked devices adversely impacting the printing services while deployed.

Another HIPS feature is the capability of application blocking which monitors applications being used by the workstation and either allows or blocks them. This feature is currently not being enforced by ONE-NET.

Host based IPS enforces a rigid access control and prevents unauthorized access, privilege escalation, joining workstations to domains, system file modifications, and changing workstation names. This restricts or completely disables the ability for the Unit IT to modify workstation configurations and obstruct the workstation integration of embarked units into the IT-21 environment using the current Embarkables mechanisms described in Chapter II.

Deficiencies in vulnerability scan results from PA. The PA tool enables the execution and scan for compliance of benchmarks such as the Federal Desktop Core Configuration or benchmarks defined with the release of IAVM notices. It also scans HBSS clients' configuration settings, compares to the previously obtained baselines and reports agent-based vulnerabilities, service misconfiguration, and policy violations. Embarked workstations and ship ePO server might have a variation of benchmarks, IAVM notices and configurations, resulting in false-positives of a policy violation reported by the PA.

Rogue System Detection: RSD sensors detect unknown systems such as workstations, servers, and printers connected to the network and lack the HBSSMA. It

sends a message to the ePO server to check in its database if the identified device has the agent installed or not. If the unidentified device does not have the HBSSMA agent, then it's considered a rogue system and an alert is created. The system can be blocked/updated with the current security policy. IT-21 RSD sensors would detect an Embarkables system as both run on different HBSS versions and would then report to the ePO server. The ePO server, also on a different version, would categorize the Embarkables unit as a rogue system and block or update it.

Embarkables work-around process: As the DoD community strives for increasing information security across all networks, HBSS implementation of policies and regulations is an additional component impeding workstation mobility across networks. HBSS client configuration and management is unique to each network and is not interoperable with other networks for the various reasons previously described. To solve this problem and allow NMCI and ONE-NET assets to integrate into IT-21, Embarkables implemented a bottom-up approach by developing a process-based solution to allow workstations to integrate into the afloat network during a deployment. This work-around ensures compliance of embarked servers and workstations while connected to IT-21 but adds extra steps, actions and possible failures for a successful embarkation.

The process requires removal and installation of HBSS by each network. NMCI and ONE-NET staffs remove any instance of HBSS into the servers and workstations configurations prior to connecting into IT-21. This allows for installation of the ship's HBSS baseline on all connecting assets. Embarked assets then connect and report thru the ship's ePO during the duration of the deployment. Upon completion of the deployment, the IT-21 HBSS baseline is removed from all assets and the NMCI and ONE-NET HBSS baselines are re-installed prior to reintegration to the native network. This labor intensive process allows support for all HBSS fielded baselines, but adds more labor and difficulties to the embarking units.

Although the current process ensures compliance with the CTO 07–12 mandate, this does not resolve the root cause of the problem. HBSS baselines are

networks specific and are not required to be interoperable with other DON networks, resulting in the emergent requirement to develop quick fixes to support the Navy's mission.

D. NETWORK BACK-END ARCHITECTURES

NNE's vision for a rapid and seamless integration of Navy and Marine Corps assets across networks by achieving common enterprise architecture faces the challenge of current divergent network infrastructures and operational environments. Key technical aspects and architectural decisions for all three networks were driven by operational environments and executed and managed by different program offices across the Navy. Such architectural decisions influenced the design of different network architectures, variations in system administration and network management services across the networks.

Leveraging the cause-and-effect diagram illustrated in Figure 12, this section identifies those operational environment factors and architectural design elements resulting in Embarkables connection problems.

1. Communication links

The most significant operational environment disparity between the ashore and the afloat networks is the wired vs. wireless connections to the NOC. Wired networks offer superior performance and reliability over Disconnected Intermittent Limited (DIL) satellite communication (SATCOM) connections as bandwidth is limited and links constantly drop. This section analyzes how the Navy SATCOM architecture influenced the afloat IT-21 architecture into what is today and how it is a major key element in the way Embarkables connect to the IT-21 environment.

By 2010, SATCOM bandwidth requirements during peacetime increased 400 percent and wartime requirements increased by 500 percent over 1995 requirements (Federation of American Scientists, 2011). These links enable the transmission of tactical and administrative data within the battle group or to the shore.

SATCOM capabilities and requirements vary per platform and mission. Navy vessels are provisioned with multiple SATCOM links and Antennas supporting line of

sight to communicate with other ships at a close distance. While in port, Navy vessels connect to the NOCs via a terrestrial line using the BLII Piers system where the system exists at the pier risers, or remain on its SATCOM connections. The Piers connection provides Fast-Ethernet (100 Mbps) speed transport services to the NOC and will increase its capacity to Gigabit-Ethernet (1 Gbps) speed commencing in FY13. Figure 16 depicts the IT-21 SATCOM and terrestrial connections.

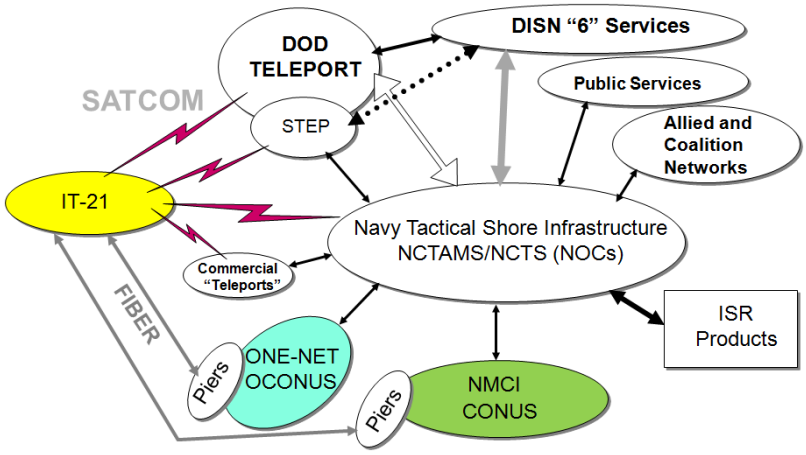

Figure 16. IT-21 Interfaces (From Smith, 2003)

During a deployment, only SATCOM links are accessible to transmit tactical, strategic and operational traffic back to the shore. SATCOM links are subject to constant environmental effects (jamming, atmospheric factors, interference, blockage, hand-over, etc.) and become disconnected and intermittent when signals expand, fade, or become limited.

Current SATCOM requirements exceed the available throughput capacity. Bandwidth limitation and the intermittent connection of SATCOM links degrades off-hull network performance; limits any system replication, synchronization, and reporting of network heath and security posture back to the shore; impacts network management requirements; disconnects any AD trusts outside the ship's boundaries; and limits or completely impedes access to certain required applications and tools.

NMCI and ONE-NET are wired networks connecting to the NOC(s) via terrestrial lines (mostly fiber), providing secure and reliable network connection with redundant

links that can be quickly employed to support net-centric services. In extreme occasions, these links get disrupted by environmental factors, but both networks have been able to maintain 99% network availability (1.68 hours downtime per week).

Wired links provide reliable, high throughput connections while SATCOM links experience severe bandwidth limitations and network performance degradation due to the intermittent connection to the shore. These operational capabilities and constraints were the primary influencers of what the current back end architectures are today and will continue influencing future architectural decisions. These facts were the main drivers for the current AD architectures and the way afloat and ashore networks receive directory services and how they are managed and sustained.

1. Directory Services - Active Directory structure

Department of Defense enforcement of authentication and authorization of users and assets is implemented by the network AD architecture and group policies. It provides centralized control and management of network resources with a single point of administration and full user access to network resources with a single sign-on using a password or smart card. AD is a central location for network administration, and is responsible for authenticating and authorizing all users and computers within a network. It administers servers, clients, peripherals and users and it serves as the focal point of the network as illustrated in Figure 17.

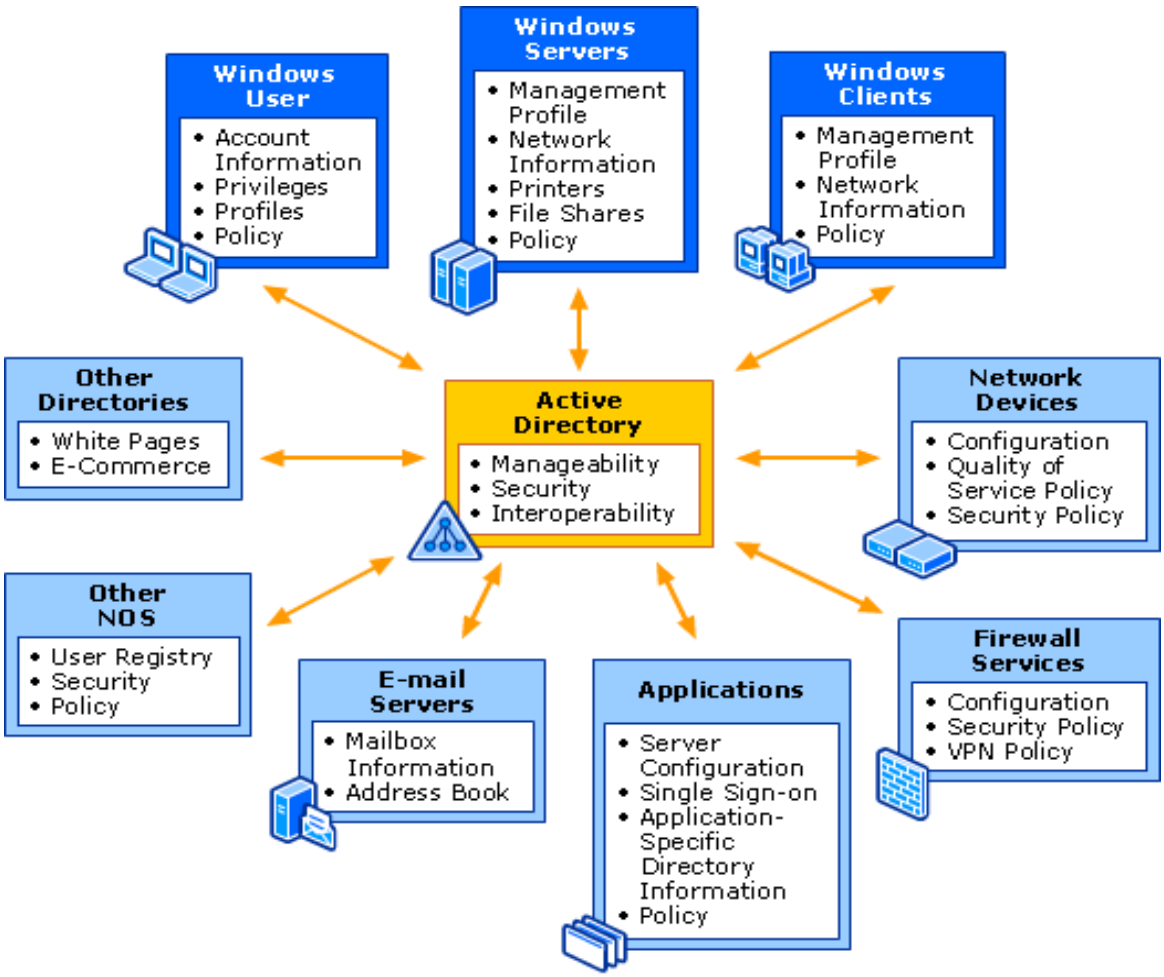

Figure 17. Active Directory on a Windows Server Network (From Microsoft Technet, 2011)

Logical topology: Windows AD organizes the networks and its objects into an organizational hierarchy of forest, trees, domains, organizational units (OU's), trust relations, and sites as illustrated in Figure 18. Forest models represent the logical structure of the network; the physical part of the network is represented by sites. Sites and forests are independent of each other, but multiple domains may appear in a single site, and multiple sites may appear in a single domain.

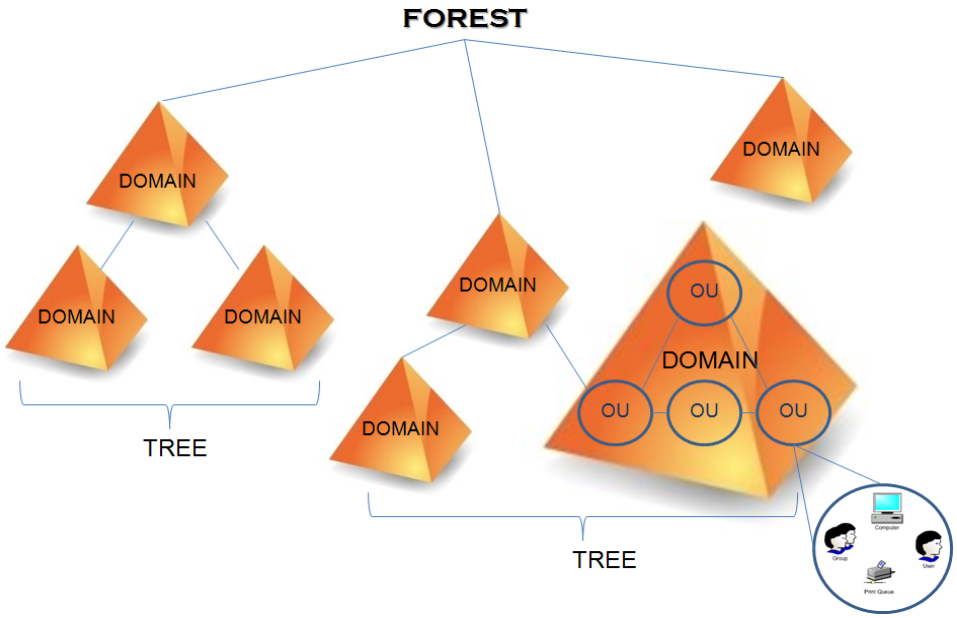

Figure 18. Logical Structure in AD (From Washburn, 2011)

A forest is a collection of one or more Windows domain trees that do not form a contiguous Domain Name Services namespace with no automatic information sharing or trusts established across forests. A domain tree is a set of AD domains that share a common namespace and are connected by an automatic transitive two-way trust. All trees in a given forest trust each other according to transitive hierarchical Kerberos trust relationships, therefore network resources can be shared between the domain trees. An AD domain defines an administrative boundary for a collection of objects that are relevant to a specific group of users on a network; each domain has a security policy that extends to all security accounts within the domain. All domains in a forest have an automatic transitive two-way trust established with all other domains in the forest. Domains are created for geographical and/or organizational structure. An OU is used to group objects (i.e. users, printers) into a logical hierarchy that best suits the needs of the organization.

Administrative Control is delegated over the objects within an OU by assigning specific permissions to users and groups (DXNET Training, 2009).

Physical topology: A site within AD represents the physical topology of the network. It usually refers to a group of computers and servers connected by high-speed

communications links. Within each site, replication of directory data between DCs is automatic. Replication between sites is less frequent and it can be controlled by systems administrators to optimize bandwidth utilization and network performance.

This AD structure allows users to move across domains or trees and be automatically authenticated to access network services such as e-mail, contacts, GAL, and network drives.

1. Ashore Networks AD structure - Single Forest Topology

NMCI implemented the Windows AD (v2.0) single forest/multiple tree model for its Navy network (the Marine network is its own forest) consisting of six domains and implemented common naming conventions and standards as defined in the AD User Object Attributes Specification released by the DoD CIO in 2005.

The Navy forest contains separate trees and domains each with their own namespace. The NMCI's DON top domain (NADS.NAVY.MIL) is an empty AD forest root domain whose primary purpose to provide namespace definition and support forest-wide administrative tasks. The two child domains are for West Coast and East Coast objects. NADSUSWE.NADS.NAVY.MIL is the West Coast domain for all USN West objects and NADSUSEA.NADS.NAVY.MILs the East Coast domain for all USN East objects; these are the primary logon domains for all NMCI users. The other domains support particular communities of interest not falling directly under DoN and are therefore outside the scope of this thesis. The unclassified NMCI forest model is depicted in Figure 19.

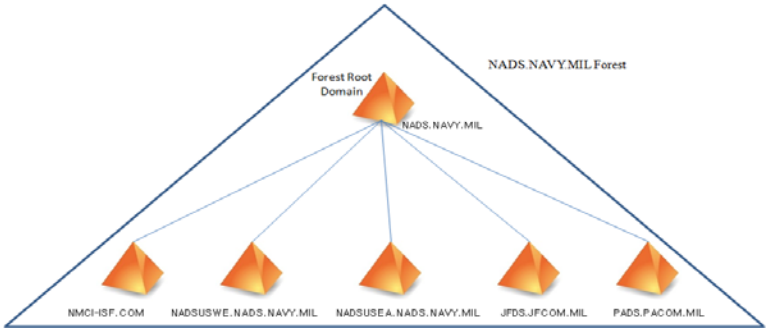

Figure 19. Unclassified NMCI Navy forest model (From Navy Marine Corps Intranet, 2010).

ONE-NET AD infrastructure consists of a single forest with two domains in a parent child relationship as shown in Figure 20. The parent domain OCONUS.NAVY.(SMIL).MIL is the forest root domain and the child domain is called DS.OCONUS.NAVY(.SMIL).MIL; this is the primary logon domain for all ONE-NET users. ONE-NET's structure was designed to mirror the NMCI AD structure. Therefore, NMCI AD is the focus of analysis with the assumption that the same concept applies to ONE-NET (Space and Naval Warfare Systems Center, 2011).

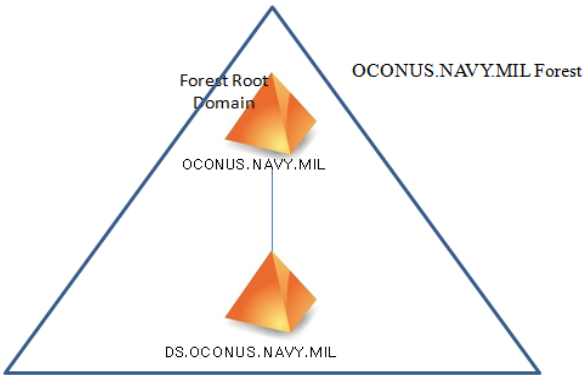

Figure 20. ONE-NET forest model (From Space and Naval Warfare Systems Center, 2011)

The NMCI model is a full mesh of shortcut trust relationships between all the domains to increase efficiencies. Shortcut trusts improve the authentication process and user logon times between domains or forests as depicted in Figure 21 (Navy Marine Corps Intranet, 2010). Two-way-trust relationship between forests was implemented between USN and USMC enclaves. External trusts are also established with ONE-NET as previously discussed in Chapter II. These TWT between networks allow for the access of host network resources while maintaining the network management capacity by the native network, including scanning for vulnerabilities and patching.

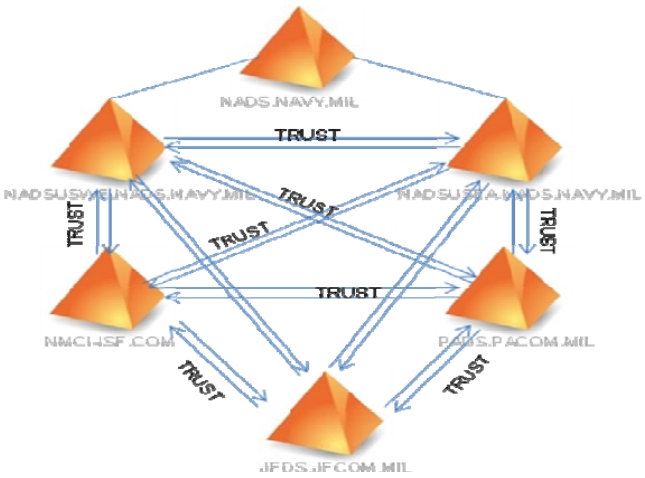

Figure 21. NMCI Navy Fully Mesh Shortcut Trust Model (From Navy Marine Corps Intranet, 2010).

Within domains, NMCI created a multilevel hierarchy of top level OU's holding multiple lower level OUs in a tier structure. The granularity of the each OU structure is based on the technical requirements or local administrative policies.

The NMCI AD enterprise structure includes a Deployable Seats OU to support workstations on deployment. As part of the Pre-Deployment process, NMCI objects from the existing OU structure in AD are moved to the Deployable Seats OU. The OU structure for deployable seats exists at the root of each child domain and is created to simplify the management of the security groups and mail-enabled contacts for e-mail forwarding purposes. Upon completion of the deployment, objects in the Deployable Seats OU are moved back to their original OU location and e-mail redirection disabled.

The rest of the root level OUs contain exchange, file and print servers; database server objects; backup and restore servers; provide security and messaging services; GPO's and distribution groups; contact's information; DHCP, Windows Internet Name Service (WINS) servers and Operational servers, groups, and service accounts.

Authentication and Authorization: Access Control and Role/Privilege Management, system functions 5.5.17 and 5.5.18 identified in Table 7 are executed by AD running on the site domain controller. It authenticates and authorizes users, groups, and computers to access objects on the network.

Upon connecting to the domain, a workstation's identity requires verification by the Local Security Authority (LSA) on the domain controller, and definition of the computer's security context, including the workstation's capability and access to network resources. These rights and permissions for a computer, user, or group are determined by Access Control Lists (ACLs) and contain security identifiers for a computer, user, or group managed by Active Directory. Other NMCI's authorization mechanisms at the enterprise include: privileges, IP restrictions, Server-Specific Permissions, Forest/Domain Modes and Functional Levels, W2K8 Domain Level Enhancements (Authentication mechanism assurance) (Navy Marine Corps Intranet, 2010).

NMCI and ONE-NET have implemented the smart card single sign-on (SSO) using credentials stored in Active Directory. SSO uses credentials collected during an interactive domain logon to allow the user to authenticate to a network one time and, thereafter, to have access to all authorized network resources without additional authentication (Microsoft Technet, 2009).

AD authenticates logon using Kerberos Key Distribution Center service and Kerberos authentication protocol as default. Authentication is performed by the DC located at the LNSC for ONE-NET authentication and at AD sites for NMCI. An NMCI AD Site meets the following criteria: (1) All NOC, Sever Farms, or micro server farm locations where domain controllers reside are defined as an AD site; and (2) Base/air station IP subnets not housing or located with DCs are assigned to the AD site of the designated SF. Several other authentication protocols are available in the NMCI Enterprise: Basic Authentication, Digest Authentication, Forms-Based Authentication, New Technology Local Area Network Manager (NTLM) Version 2, Kerberos Version 5, X.509 Certificate, and Internet Protocol Security. There is no default authentication protocol identified by NMCI, but Kerberos Version 5 was listed as the preferred mechanism (Navy Marine Corps Intranet, 2010). ONE-NET uses CAC for front-end authentication, and uses Kerberos, Version 5 as the default back-end authentication mechanism.

The Local Security Authority is responsible for all interactive user authentication and authorization services on a local computer. Each AD object is protected by access

control entries that identify which users or groups can access that object and defines what level of access is allowed. NMCI and ONE-NET AD include root-level OUs at each domain for Access Control Authentication to hold and manage workstations and printers.

2. Afloat Networks AD Structure - Multiple Forest Topology

IT-21 implemented a multiple forest structure where each ship is its own AD forest due to the bandwidth limitations and problems with continuity of communications between ships and shore. Each ship is entrusted to maintain its AD schema and to maintain compliance with the guidance provided by the PEO. This guidance on AD naming standards and schema was designed to mirror the NMCI naming standards as closely as possible.

A multiple-forest topology provides messaging service and data isolation, including Exchange, which is a requirement for the IT-21 SATCOM environment due to the intermittent connections. It establishes strict boundaries between ships' forests and therefore provides a more secure environment than a single forest topology. The IT-21 AD forest model is illustrated in Figure 22.

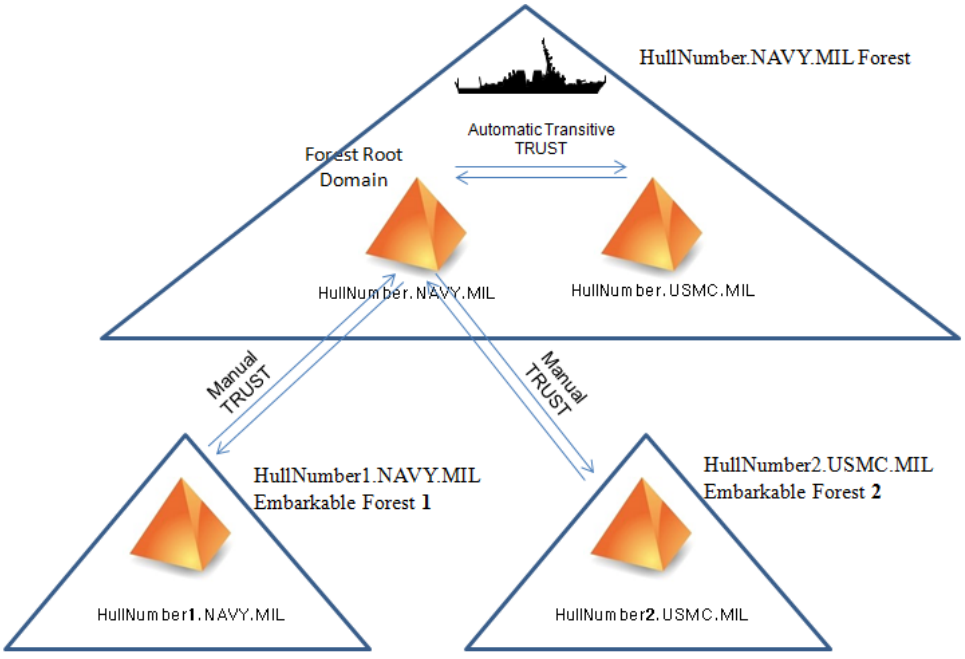

Figure 22. Example IT-21 AD forest model including a Embarkables forests objects (From Net-Centric Geospatial-Intelligence Discovery Services, 2002)

AD namespace includes the hull number such as HULLNUMBER.NAVY.(SMIL).MIL for the ISNS domain (other domains compose the IT-21 environments such as SubLAN and SCI). Within the domain, a hierarchical OU structure holds all domain objects (Net-Centric Geospatial-Intelligence Discovery Services, 2002).

Authentication: IT-21 has not implemented the smart card logon and it provides domain user ID and password authentication capability via workstations to control end-user access to network domain resources. The user logon name must be unique across the entire Navy and USMC enterprise. Users' logon interactions are managed by a secure process called Winlogon. The LSA receives the user name and password from Winlogon and determines whether the logon process is to be authenticated on the local computer or across the network as a domain account and the Kerberos authentication package on the domain controller validates the user. IT-21 users do not use CAC logon but utilize CAC credentials to access PKI enabled websites such as Defense Connect Online (DCO).

3. Directory Services and Embarkables.

AD architecture design was primarily driven by the operational environment and requirements for each network, where deployed ships' communications must be able to function in isolation due to the low WAN throughput intermittent satellite links connecting to the shore. User and workstation mobility across these two different architecture structures cause loss or degradation of the following services and capabilities:

Authentication- NMCI and ONE-NET domain authentication is not available for Embarkables during a deployment because the DCs reside at the LNSC and there is no AD trust between shore DCs and ship DCs. Therefore, an IT-21 domain account must be created for users and workstations and must be added to an IT-21 forest. The PPS suite includes two domain controllers (for redundancy) to support directory services provided to the Embarking units, including user logon processes, user authentication, and client security policies. The IT-21 domain controllers perform authentication for embarked

users without PPS. The AD structure at the ship's root domain includes an Embarkables OU to add users and client accounts for embarking personnel without PPS.

Outlook services - Users with e-mail redirection to their IT-21 e-mail account cannot access the NMCI or ONE-NET global address books, contacts or calendar sharing. There is no access to other IT-21 GALs. Internally to IT-21, other ship address books are not accessible and address book sharing must be coordinated and obtained via shore.

Embarking units cannot encrypt or sign outgoing e-mail during deployment because their CAC e-mail certificate does not match the IT-21 e-mail account being used.

Security - Workstation security posture is lost over time while workstations are not connected to their native network, automated patching management is disabled and security policies are not updated to maintain compliance. Unit IT or ship's staff needs to ensure that workstations receive security patches.

Users and workstations lose role based capabilities, drive mappings and any other settings on a GPO appropriate to the workstation and logged on user, as the group policy client on the machine won't be able to access and pull any refresh settings.

Printing - Printing capabilities to network printers are available through the TWT with the ship's forest. Some limitations do exist to Embarkables assets due to the HIPS policies implanted not allowing access to locally shared printers, widely used on the IT-21 environment due to the LAN drop limitations.

Desktop - AD locks down desktops using Group Policies for NMCI, ONE-NET and IT-21. Software installation, configuration and updates for Embarkables units must be manual loads, as the software distribution agents are disabled during deployment and no other software or patch distribution methods are allowed. Non-baseline software requires approval and security compliance prior to installation.

AD provides all mailbox information, GAL services, and other recipient-related information, therefore the divergent AD structures on the ashore and the afloat networks

make it practically impossible to move across network without major reconfiguration at the front and back end of the network (Microsoft Technet, 2005).

E. CLIENT IMAGE

IT-21, NMCI and ONE-NET implemented standardized COTS and GOTS software bundles, referred to as workstation images, to deliver directory services and applications to network clients. A workstation image is a copy of the entire state of the system stored in some non-violate form, allowing the image to be restored exactly in the same state after a system shut down. Every workstation requires a unique identity within each network. The naming convention is unique for each network and enclave and to distinguish between desktops and portable workstations. These naming conventions allow scripts to accurately target certain users and devices.

Each network workstation image software bundle consists of seven possible software/application categories: (1) core software; (2) security and information assurance software; (3) business management applications; (4) media players and file viewer; (5) enterprise software management; (6) collaborative tools; and (7) above core applications.

Core software includes the operating system, web browser and Microsoft software framework. Security and information assurance software include DAR products, Antivirus, HBSS agents and the latest security upgrades. Business management applications consist of Microsoft Office products. Media player and file viewer software include: Adobe file viewers, Apple's QuickTime Player, and Microsoft Media Player. Enterprise software management includes SCCM, Tivoli, Radia. Collaborative tools include chat, conferencing, and messaging tools such as NetMeeting and Mako chat client. Above baseline applications are many but some examples are: Microsoft Project and Visio, Adobe Professional, AutoCad, Naval Aviation Logistics Command Management Information System (NALCOMIS) and IBM's MAXIMO which are applications for certain commands or user groups but not part of the image baseline.

IT-21 client core build is the COMPOSE versions 2.0.3, 3.0.0, 3.0.1, 3.5.0 to 4.0.0 supporting WIN XP Service Pack 3 (SP 3) and Windows 7 SP1. The NMCI Core Build is the complete set of core applications for a particular platform and OS. NMCI currently

supports WIN XP SP3 and WIN7 SP1 (Hewlett-Packard Development Company, 2011). The ONE-NET standardized desktop configuration is called the Workstation Baseline Software Configuration (WBSC) and the current version is 118, which is based on WIN XP SP3.

The three networks operate on Microsoft Windows platforms WIN XP SP3 and WIN 7 SP1 operating systems. Upon release of an new image for NMCI and ONE-NET and to validate compatibility with the fielded image due to the continuous updates, the IT-21 tests that image on it's COMPOSE environment to ensure functionally.

Software and applications in most categories are tied to network resources or vary in software product resulting in software and image incompatibility: (1) IA software and enterprise management client agents pointing to specific servers for security updates to maintain the image compliance such as DAR and HBSS; (2) security template settings on workstations based on DISA policies to ensure compliance and maintain network security posture vary for each network; (3) variation of Antivirus solutions, IT-21 on Symantec Antivirus v10 (SAV 10), NMCI on Symantec Endpoint Protection v11 (SEP 11), and ONE-NET on McAfee; (4) above baseline applications pointing to servers such as MAXIMO and NALCOMIS which is a critical logistics application to log plane and flight information; (5) baseline applications pointing to a server (Internet Explorer pointing to different proxy server); and (6) floating licensing software pointing to a license manger on the network, such AutoCAD used by the Naval Facilities Command reaching out to the FlexLM server located at the ONE-NET's TNOSC in Japan.

PMW-160 is currently utilizing virtualization technology to build multi-image workstations with NMCI, ONE-NET and ISNS (COMPOSE 4.0) loaded to seamlessly connect and operate on all three networks. Workstations would then seamlessly connect and be centrally managed and maintained on the network they are connecting to.

F. CHAPTER SUMMARY

This chapter explored the factors contributing to the Embarkables inability to seamlessly connect into a visitor network and obtain IT services without configuration requirements at the desktop or network level. By identifying the functionally loss or

degradation during a deployment, and mapping those functions to system components, it is identified that network management and the back end architecture are the primary causes for Embarkables integration problems.

Patch management deficiencies and functionality issues with the security related solutions are directly caused by the variation of management tool and products, and processes used to monitor, manage and sustain the network. A deep analysis was performed on patch management to identify the root causes for inability of Embarkables to receive patches while connected to IT-21. The Ishikawa diagram identified four major categories which can be applied to most interoperability issues between the ashore to afloat networks: (1) Equipment (Management tool), (2) Environment (Architecture), (3) Process and (4) People. The decentralized network management IT-21 model; the variation and incompatibility of management tools; the different desktop images requiring different patches specifically packaged to be deployed by their corresponding patching tools; and the manual process to download patches via SATCOM resulting in high failure rate are the primary causes for patching problems during deployments. The AD structures between afloat and ashore networks is significantly different. Single AD forest vs. Multiple AD forests with no trust to any other forest maintains each ship in isolation. Although it is required for IT-21 to be self-sustained while at sea, this isolation prevents any data sharing, replication, and collaboration with other IT-21 ships or ashore.

Current networks are not flexible or adaptable; they were designed to optimize performance for each unique environment but were not designed to integrate with other networks while optimizing the overall performance of the system of systems. Consequently, the PEOs develop and continue improving bottom-up solutions for net-centric communications to enable IT services to ashore users while deployed on an IT-21 environment. These processes and initiatives are interim solutions to afloat and ashore network interoperability problems but do not fix the root cause of the problem.

IV. RECOMMENDATIONS

A. INTRODUCTION

This chapter presents high level recommendations for the existing Embarkables process to facilitate integration into the IT-21 environment for services, and consequently minimize the embarking user's downtime. Additional recommendations based on successful implementation of IT solutions by the private sector to support mobile and remote users are explored in this chapter as viable alternatives for the Navy's mobile IT services requirements.

B. IMPROVING CURRENT EMBARKABLES SOLUTIONS

The operational environment of Navy ships requires the network's ability to achieve and sustain self-sufficiency while in a deployment status when SATCOM connectivity is lost. While SATCOM links constantly increase in capacity and reliability, the demand for bandwidth exceeds the throughput SATCOM links can supply. Exploring solutions to alleviate and improve the Embarkables' integration into the afloat network must keep this operational limitation into consideration and should focus on keeping SATCOM requirements to the minimum while providing Embarking units the IT services required to complete their mission during a deployment.

1. Ashore Solutions to be Tested against the Embarkables Process

Although ONE-NET and IT-21 develop networks solutions, naming standards and architecture decisions to mirror NMCI as much as possible, there is no interoperability requirement for any network. In more recent years, Navy networks have leveraged each other's IT solutions when feasible, as part of the network realignment efforts: ONE-NET's DAR design was based on NMCI's solution, AD IT-21 and ONE-NET leverage the NMCI naming standards and guidance, and NMCI and ONE-NET HBSS solutions are same product line and similar policies have been implemented.

Despite this collaboration among Navy networks and similarities in some solutions, there is no formal process to validate functionality of solutions across

networks. New solutions are tested against their own network and fielded to the enterprise without an Embarkables' evaluation on technical and/or programmatic risks. There is no requirement to test new solutions against the Embarkables integration process, or to evaluate the impact of the new solution on workstation's performance during deployment. Solutions are fielded to the enterprise without an Embarkables' validation test. As a result, integration issues are identified in real time during a deployment, requiring immediate technical support and reverse engineering to indentify the root cause of the problem to resolve the issue and integrate the seats into IT-21.

Incorporating the Embarkables team into the development and testing of any enterprise solution would facilitate the early detection of interoperability problems due to technology gaps, processes or implementation of security rules and policies. The Embarkables team should be engaged with the engineering team to modify the technical aspects of the design, or work with the proper authority for policy waivers or modifications to prevent integration problems.

Testing solutions in the IT-21 network prior to fielding would identify most issues in a lab environment when there is no impact to the user. Adding interoperability verification as part of the test and evaluation process for every solution would identify any interoperability problems in a timely manner prior to fielding to the operational environment.

IT-21 is currently piloting the WSUS patch management process. This process eliminates the manual selection and download of patches for the COMPOSE environment and could be leveraged for the patching of Embarkables seats and saving man-hours. While it's in its pilot phases, there is no requirement to test for Embarkables seats; therefore no testing has been performed.

2. Leverage Existing DoD Solutions for Mobile Networks

NMCI deployed the DSTB solution to support mobile Navy and Marine units on remote locations while providing bandwidth optimization over high-latency and unstable

WAN circuits. DSTB provides VPN over IPSEC encrypted traffic over multiple external networks and delivers “office-like” connectivity to mobile users (Navy Marine Corps Intranet, 2011)

DSTB is a small footprint on the host network, requires one power outlet, one public IP address, and WAN and LAN connections. It consists of: one outer router which connects to the inbound circuit; one inner router supporting 48 connections; one VPN Device; one WAN Accelerator which improves bandwidth performance up to 60%; and an uninterruptible power supply for non-permanent installations in a durable case (Wolff, 2008). Enhancing the DSTB with a server farm to include file, print and e-mail services would allow ashore assets to operate onboard ship with little or no integration. The DSTB solution has been deployed by NMCI for permanent or semi permanent deployments, and to support exercises and administrate deployments for 90 days or less. For each instance, an accreditation package is submitted, reviewed and approved by the ODAA to validate that the system is meeting all security and accreditation policies and requirements.

DSTB provides the transport capability for the network by connecting to NMCI via a secure VPN. This connection requires continuous access to a SATCOM link to maintain the VPN tunnel and traffic flow in and out of the ship for e-mail, Internet access, application access, or any other required service. The ship’s limited bandwidth links cannot support this persistent VPN connection for the Embarkables traffic flow to the shore. Some of the required IT services must be provided within the ship to minimize bandwidth requirements over SATCOM. The PPS suite, currently used by the Airwings and some Marine units, provides the data storage capacity, exchange and domain controllers needed to provide basic services to the embarking unit.

Using the PPS with NAS and the enhanced DSTB, users can maintain their native network e-mail and GAL, digital e-mail signature capability, CLO, home drives; assure access to command shared data, and be assured that the distribution of enterprise services and IA security requirements will be maintained during the deployment. The PPS and DSTB server farm allow the embarking units to be self-sufficient during SATCOM

downtime since network resources remain within the skin of the ship and the DSTB allows reaching out to the NMCI environment when SATCOM is available.

Deployment missions often require direct collaboration across other embarked commands and access to ship resources. This requires the creation of a TWT between the DSTB and the ship's domain; it would allow the use of ship's resources such as printing, proxy services, and connection to ship hosted applications such as NALCOMIS for aviation logistic information.

The DSTB solution is currently not used on the IT-21 environment. The primary concerns for implementing the DSTB to support Embarkables are the bandwidth requirements and the initial fielding cost. The author developed a four year cost estimate profile for the acquisition and maintenance of one DSTB System utilizing known initial hardware cost, fielding and yearly maintenance costs (Weatherspoon, 2010). Inflation data rates and normalized cost estimates to Then-Year dollars (TY$) were used to represent the actual cost that can be expected the year the dollars will be expended as illustrated in Figure 23.

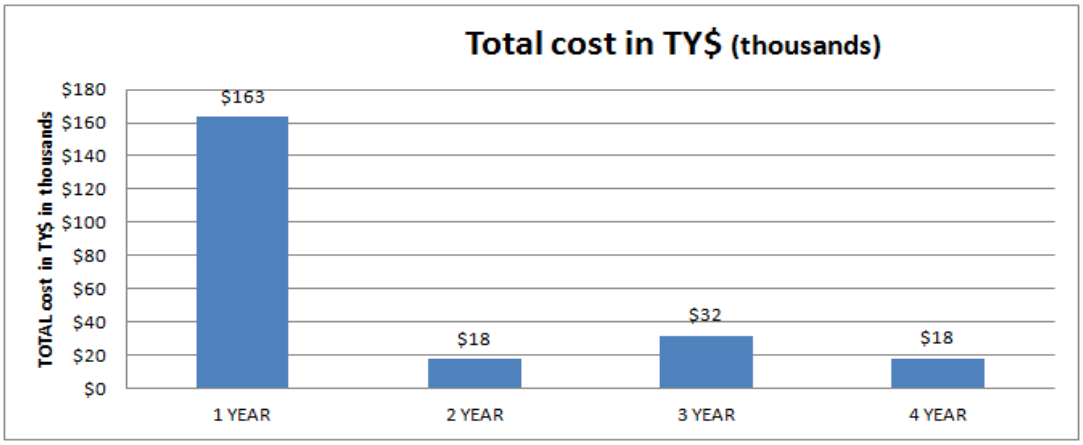

Figure 23. DSTB Four Year Cost Estimate

This cost profile is based on a DSTB life cycle sample of four years with initial acquisition in FY12 ($127,538); assuming 6 month deployments; two deployments on even years and one deployment on odd years starting in FY12; one time technical support per deployment ($13,000); monthly IAVA support throughout the year ($303 per month);

and utilizing the DoD Inflation rates provided by the Office of the Secretary of Defense Program Analysis and Evaluation. This cost does not include system accreditation cost, or any cost incurred on the ship network services such as bandwidth utilization. Total life cycle cost in FY12 dollars is: $228,621.

A comparison between the total cost to field and operate a DSTB system, and cost to associated with the man-hours required to integrate the same amount of Embarkables assets during a four year period demonstrate substantial savings to the Navy: a common deployment consists of a Commander Air Group with 50 seats and a Commander Carrier Strike Group with 800 seats per deployment, totaling 850 users. On average, the Unit IT spends 45 minutes per seat (Weatherspoon, 2010). Per deployment, it takes the Unit IT an average of 635 hours per deployment. Considering a 4 year period (assuming DSTB refresh on the 5th year), and assuming six deployments during the 4 year period, the total man-hour savings are approximately 3,800 hours, not including the time to create an Embarkables domain, user accounts, redirection of e-mail, and reintegration back into its native network which very often requires the reimagining of the workstations.

In addition to cost associated with using DSTB on the afloat environment, there are other technical considerations that would need to be further analyzed and tested: data storage requirements, shipboard bandwidth impact, data store synchronization requirements, exchange synchronization requirements, operational deployments procedures, DSTB technical upgrades, firewall security requirements, and solution performance metrics (Rivera, Streamlined Embarkables, 2010).

Additional considerations are the AD latency tolerance and VPN performance over SATCOM. The maximum latency for a reliable IPSEC VPN tunnel between the DSTB and NMCI is 600ms Round Trip Time (RTT). Exceeding this maximum latency will result in failed connection between DSTB and the ashore network. Typical RTT for cross-country or trans-oceanic land-based WAN links are normally in the range of 100 to 200ms, yet a satellite link is 500ms RTT. Factoring in other normal delays from network sources could increase this latency beyond the 600ms for the IPSEC tunnel resulting in constant loss of VPN connection (Kruse, 1995). As the Navy operates in areas of the

world where bandwidth is extremely scarce and expensive, DSTB bandwidth requirements, cost, impact on ship communications and it associated benefits and risks need an in-depth study and evaluation.

3. Enterprise Services for Seamless User Experience

In the new cyber era ruled by the concept to provide services from a cloud, why not utilize the cloud to service military forces deployed anywhere in the world?

Exchanging e-mail messages has evolved to a fast, reliable, real time communication method among physically dispersed users and across networks, increasing organizational productivity and profitability. The DoD has become dependent on e-mail for communication and information sharing at different security levels, enclaves and across military branches.

Standardizing into a single common Navy e-mail would facilitate the ability to seamlessly exchange electronic messages and transition between environments during deployment and from anywhere in the world. Achieving a single e-mail model will require reengineering the network, fixing the back end architecture considering the current constraints, or will require deploying an Off-The-Shelf (COTS) plug in solution. While these alternatives represent programmatic and technical challenges, it is essential that a system engineering approach is implemented at every phase of the life cycle of the system in order to design, build, deploy and maintain the right product at the right cost.

This section provides an overview of some industry and commercial cloud-based solutions that could be used as the basis for a new Navy e-mail service model.

a. Cloud-Based E-Mail

Cloud-based e-mail means outsourcing e-mail service in its entirety to a cloud-based provider including hardware, software updates and licensing, security and patching. Outsourcing e-mail services minimize the e-mail footprint; reduce administration cost; facilitates user mobility; and allows organization tier structure, to tailor e-mail accounts to user needs including: mailbox size, mobile messaging, message filtering, licensing and updates. The cloud-based concept is illustrated in Figure 24.

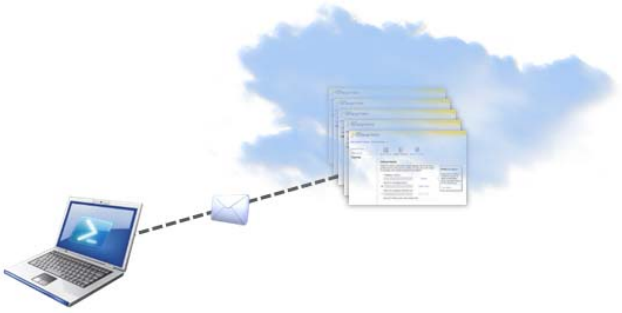

Figure 24. Cloud-Based e-mail (From Microsoft Technet, 2010)

A Forrester report published in 2009, reveals web based e-mail has much lower cost than e-mail with an on-premise e-mail client. On-premise e-mail costs a company $302.16 per user/year compared to roughly $50 per user/year the U.S. Army will be paying the first year of transitioning to a cloud e-mail service (this cost is expected to decrease after the first year of service) (Serbu, 2011). The major cost difference is the storage growth fees, archiving, mobile access, equipment failures, staffing, provisioning, and ongoing maintenance costs.

Some of benefits of cloud-based e-mail include a more predictable and manageable storage cost generally charged on a flat per user, per month basis; no initial upfront commitments for infrastructure, hardware or licensing, and lower ongoing IT costs; a easy and fast deployment time; full redundancy and 99.99% network availability; transparent, continuous top-of-the-line upgrades; scalability; built in antivirus and anti-spam protection; e-mail access anytime, anywhere from any authorized, CAC-equipped computer; only pay for what is used; and easy administrative web based control tools. To the end user, an enterprise e-mail would allow mailbox, contacts and GAL access anywhere in the world and from any network.

Outsourcing the control and management of tactical military data to third parties on the cloud would result in loss of full control over data and processes and this lost is one of the primary roadblocks for the Navy to move its data to the cloud. The decision to implement outsourcing requires a trade off analysis between security and cost.

b. Hybrid E-Mail Model

On-premises messaging and cloud-base e-mail are not mutually exclusive; they can co-exist to provide organizations with an optimized solution to meet its specific needs. A hybrid solution is a combination of services provided by an on-premise e-mails system augmented with the cloud. The model must be customized based on what makes security, cost and technical sense.

There are two main hybrid combinations: First, some e-mail services run on-premise and some run in the cloud; mailboxes remain on-premise and the archiving, management, and inbound e-mail spam and virus filtering are moved to the cloud.

Second, some users run on-premise and some run in the cloud; this hybrid model is designed to meet the needs of a diverse workforce by customizing user accounts and only providing what each user needs. It uses a tiered workforce model with three categories: mobile executives who need big mailboxes and mobile messaging (such as Embarkables users); information workers who need a dedicated e-mail client (most NMCI and ONE-NET users), but smaller mailboxes; and occasional users who don't need big mailboxes or dedicated e-mail clients (IT-21 users) (Schadler, 2009). This model brings the ability to move mailboxes from the cloud to on-premise servers as needed. The ability to move mailboxes from the on-premise to the cloud and back allows Embarkables users to maintain their e-mail during and after deployments.

Figure 25 illustrates a hybrid model using exchange on-premise service for mobile executives and information workers and cloud e-mail for occasional workers.

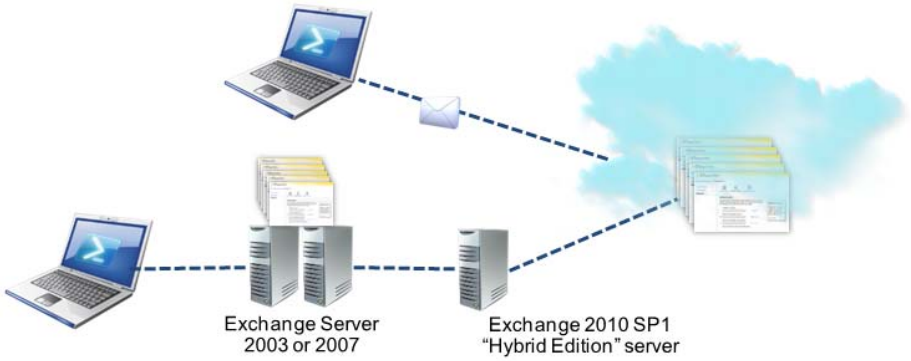

Figure 25. Hybrid e-mail model example (From Microsoft Technet, 2010)

Hybrid e-mail introduces challenges of its own: e-mail features may differ for cloud and on-premise mailboxes; hybrid e-mail adds complexity in managing compliance; challenges in seeing "free/busy" status on calendars in the other domain; administrative challenges; no GAL segmentation or hierarchical address book; no multiple on-premise AD forest; no public folders; and no OWA login capability (Schadler, 2009).

Outsourcing e-mail services is not new to the DoD. In 2011, the U.S. Army began transitioning over 900,000 users to a DISA cloud for e-mail services. Some DISA cloud's benefits include providing CAC authentication, sending e-mails with larger attachments than is currently allowed, providing 4 gigabytes of online e-mail storage for standard e-mail account holders, and 500 megabyte webmail accounts for those who don't normally use Army e-mail to perform their duties (U.S. Army, 2011).

E-mail is a mission critical application for any organization, including the DoD. Developing a cloud-based standardized Navy's e-mail solution requires a top-to-bottom design approach and the implementation of systems engineering techniques including functional decomposition of all system requirements, traceability of functions down to system components to prevent any gaps or overlaps, regular stakeholder inputs and milestone reviews, and requirement validation to obtain the best solution possible.

C. CHAPTER SUMMARY

The Navy has made some key architectural decisions which have shaped the current network architecture, AD structure and Navy's business portfolio based on the operational environment, requirements and constraints. As new emergent challenges and requirements drive the increased the complexity of the Navy's operations, the PEO must better utilize current solutions and explore new technologies to meet the dynamic requirements while balancing cost, schedule and performance.

Leveraging and enhancing NMCI's DSTB, PPS and two-way-trusts to develop an office-like solution to embarking units while accessing network solutions has its technical, programmatic and cost challenges but is a possible interim solution to the

problem of rapidly and seamlessly integrating embarking commands into IT-21, enhancing command productivity and efficiency.

The author recommends further exploring new technologies such as hybrid e-mail, an evolving technology which has reached a mature state and has proved to be efficient and has resulted in cost savings to the private sector.

V. CONCLUSION

A. INTRODUCTION

> "The mission of the Navy is to maintain, train and equip combat-ready Naval forces capable of winning wars, deterring aggression and maintaining freedom of the seas."
>
> —Mission statement of the United States Navy

Over 320,000 Navy active duty men and women and over 200,000 U.S. Marines serve this country and protect America and its citizens at home and abroad (Department of Defense Manpower Data Center, 2011). Their duty is to defend our freedom, maintain peace, provide relief and support policies around the world by rapidly and effectively responding to evolving threats to our national security by air, land, sea and cyber space.

Approximately 67,000 of Navy members serve onboard ships, supporting Marine units and Airwings during scheduled and unscheduled deployments around the world. Identifying, preventing and promptly responding to any acts of war are imperative to protect the American people and assets around. This requires the ability to rapidly deploy military forces and effectively integrate into any environment, thus increasing information technology capability and enhancing mission effectiveness.

As the Navy strives for network commonalty and alignment, immediate capabilities are needed to support deploying forces anytime, anywhere in the world. The deployables' mission is to provide mobile Navy and Marine assets the ability to interoperate on diverse networks in multiple deployment scenarios (Rivera, Deployables STEAG Brief, 2009). The diversity of operational environments and the embarking commands result in Embarkables integration problems.

This thesis analyzed the different Embarkables processes and identified contributing factors to the interoperability problems experienced by the Embarkables assets while integrating into the IT-21 environment. These findings are summarized in this chapter by answering the research questions, followed by final comments by the author at the conclusion of this chapter.

B. ANSWERS TO RESEARCH QUESTIONS

1. What are Embarkables and What are the Challenges They Currently Face?

Embarkables are the Navy and Marine assets, users and workstations, deploying from NMIC, ONE-NET and other ashore networks and integrating into the IT-21 network. This thesis focused on NMIC and ONE-NET Embarkables only, other network assets connecting to the IT-21 environment were not considered in this research.

The Embarkables requirements vary for each network: NMCI deploys to IT-21 and ONE-NET, ONE-NET deploys to IT-21, and IT-21 does not deploy to any network but supports integration of assets coming from the other two networks. The Embarkables mechanisms (also called Deployables) facilitate asset mobility between these networks but require complex and time consuming IT processes to integrate into the IT-21 network's topology due to interoperability deficiencies and lack of trusted relationships between the networks. Chapter II provided an overview of all Embarkables mechanisms currently employed by the Navy and Marines. Some of the challenges currently faced by these Embarkables mechanisms and the embarking users and workstations are:

Lack of defined requirements for Embarkables: A composed list of clear Embarkables requirements and measurable performance thresholds was not found. Requirements are defined at a very high level in the NMCI contract but are not specific enough to develop an enterprise solution. Therefore, PMW-205 and PMW-160 developed ground rules and Embarkables mechanisms to integrate ashore assets into the afloat environment. These processes were tailored by each region and by each network. Undefined and unclear requirements leave room for a technology and architecture variations and implementation of solutions.

No requirement to test new solutions against Embarkables: Although networks leverage each other's network solutions in terms of technology and design when feasible, they are not required to test and verify interoperability between networks. Due to this lack of interoperability testing requirements, network solutions are

engineered, tested and fielded without inputs from the Embarkables community, and without notification to the IT-21 network that a new solution has been deployed which could potentially impact asset integration. It is common that during a deployment, the recently fielded solutions causes seat integration issues and the Unit IT, the Embarkables support team, and ship's staff struggle identifying and fixing these issues in a timely manner.

Variations in the Embarkables process: Variations in the end-to-end Embarkables processes generate ongoing challenges due to inconsistencies in workstations' readiness state to integrate, differences in capabilities, by command or by embarking unit, in network servers and storage capabilities , insufficient unit IT support for the size of the embarking command or IT staff unfamiliarity with the process. At times, the Marines leverage the permanently installed and pre-configured PPS suite as part of the ship's forest, and at other times they bring their own servers suite. The Airwings bring their own Embarkables server and are provided their own forest. Other users embark without a server suite and connect directly into the ISNS system. NMCI and ONE-NET have automated some part of the Embarkables processes by deploying the DMT. Although NMCI and ONE-NET DMT tools provide similar functions, they provide a variation of capabilities to the Unit IT and the end user resulting in variation of the pre-deployment process and provide different level of visibility of the Embarkables assets to the Unit IT's.

Seat integration a time consuming process: Though Embarkables processes were partially automated with the introduction of the DMT, they have failed to keep up with the fast deployment of new solutions by the ashore networks. Some of these solutions impede and limit asset integration into the IT-21 environment, such as HBSS, and remain a labor intensive and time consuming integration procedure. The average time spent integrating an ashore seat into IT-21 is 45 minutes, assuming no problems, and does not include the intensive workload and time consuming coordination prior to each deployment.

Commands unfamiliar with the Embarkables process: Commands that do not normally deploy and are unfamiliar to the deployables process, sometimes attempt to

bring equipment not listed in the IT-21 ISNS Preferred Products List (PPL) and that not are allowed to be integrated into the LAN. Many times those commands embark without a Unit IT for support, therefore depending on the already busy ship's staff for IT assistance. This gives the perception that the Embarkables processes are broken and potentially results in negative advertisement.

2. What are the Requirements for the Deployed Users/Systems for each Network?

Other than high level requirements on the NMCI contract, there are no specific requirements on what IT services or capabilities Embarkables assets must obtain during a deployment. Solutions were developed and implemented to support the war fighter assuming a 'seamless' user experience when connecting to IT-21. Chapter II identified all services obtained by users when connected to their native network. These services were compared to the services received during a deployment for three different scenarios represented by user cases. Using the most common scenario, when embarking unit brings storage servers onboard, the IT services were grouped based on availability when connecting to the ship's network.

Seamlessly obtained services and capabilities during a deployment are limited to: the ability to logon to the local workstation, access MS Office and other applications previously loaded on workstation, access to hard drive data including e-mail archives and .pst files, and the ability to copy files to external media and reproduce CD/DVDs.

Services and capabilities that require network reconfiguration or depend on the host network to function included most of the IT services: network access, e-mail and calendar capabilities, print/scan/fax, chat, access to home drives, command share data and portals, VTC, and file transfer. Other functions transparent to the end user but required to maintain seat security posture include: OS and application patching, backup and restore capabilities, remotely receive applications, and push of required security policies.

Other services and capabilities that are completely lost throughout the deployment period include: access to home network GAL and contacts, ability to digitally sign e-mail and access to public folders.

Based on the gaps of services available during deployment, a function-to-component traceability matrix was performed to identify possible root causes of those problems, further explained in the following research questions.

3. What is the Impact of Different Desktop Configurations?

Afloat and ashore networks have customized Windows-based images which are not compatible with each other. Each desktop image baseline includes above core applications which are unique for the environment each network supports; business management applications which are mostly COTS and therefore compatible; enterprise software management agents which are different and incompatible among the three networks; and security and information assurance software such as an IA required Antivirus solution, for which each network runs a different product.

Network management agents point to specific servers, such as the network patch repository and to the ePO server for HBSS, to obtain security updates and maintain desktop image compliance. These agents constantly access the patch repositories for latest OS and application patches to remediate network vulnerabilities to abide by DISA policies. These agents must be disabled during deployment, halting the ability to receive patches remotely from their native network. These seats must leverage the IT-21 patching process when feasible or perform manual patching throughout the duration of the deployment.

Although NMCI and ONE-NET workstations have their own network image, they are capable of joining the ISNS domain and stay connected without having to be reimaged with the COMPOSE load. They do require to be manually joined to the Embarkables domain, to have proxy and exchange settings point to the ship's servers, and have settings reconfigured to receive patches according to the patch management process used on the ship.

4. What are the Network Management and Architectural Differences?

By performing a functional decomposition, function-to-component traceability matrix and an Ishikawa diagram, the following network management and architectural differences were identified:

Variation in network management tools: Each network uses different vendor tools which are not compatible among themselves. These tools were selected due to the difference in operational requirements: (1) IT-21 tool does not need to support tiered network architecture or to patch non-Windows servers, while NMCI and ONE-NET do; (2) ONE-NET has a requirement to minimize the amount of agents installed on a seat to perform multiple management functions and the requirement for a scalable of product; (3) NMCI had a requirement to obtain user authorization for remote control of workstation which led to the use of an additional tool, NetMeeting.

These additional requirements for the ashore networks led to the selection for Radia for NMCI and Tivoli for ONE-NET. IT-21 selected SCCM, the least complex and most cost effective solution (at the time of selection) to manage their network.

Security compliance by network management and implementation of policies are incompatible: An important element of network management is patch management. This thesis identified the different patch management processes and the possible contributing factors to the inability of workstations to be seamlessly patched and the current issues the Embarkables face to get patches during deployment. During the brainstorming process to identify potential root causes leading to the problem (effect), major causes were broken down into sub-causes to identify relationships between the effect and all the possible causes directly or indirectly influencing the outcome. The following sub-causes are influences in most of the major categories: dissimilar AD structures; management tool interoperability; different processes; and undefined requirements.

Deeper analysis into the patch challenges identified that the manual download of afloat patches during deployment is one of the causes of the inability to patch Embarkables seats: the size of patches is too big to download via SATCOM; low

bandwidth, high latency and intermittent connection causes patch downloads to fail; Unit IT must manually search for patches that apply to the Embarkables seats which is time consuming and could result in the wrong patch attempting to be applied; the U-Patch utility is available to NMCI seats for patching but still requires the manual download of patches into the source directory and initial configuration of all workstations to point to this source directory; and onboard LAN traffic is also limited, therefore distributing patches onboard the ship is limited to few seats at a time.

Upon completion of the deployment, the assets must be up to baseline to reintegrate into the native network. Rather than verifying that all patches are up to date and that only approved applications are loaded on each workstations by performing visual inspection and comparing to image information for that each specific seat, some ashore commands opt to reimage the workstations prior to allowing them to re-join their home network.

Directory services structures: NMCI and ONE-NET directory services structures share similarities as both are composed of centralized active directory services for domain management, with logical structure of one forest for the entire enterprise, with trees and domains in a similar hierarchical organization and domain meshed models. Deploying multiple domain controllers in one domain provides fault tolerance and load balancing so failover capabilities provide enterprise support if a DC slows, stops, or fails since they contain the same directory data. This model provides centralized identification and authentication control allowing user mobility between logical and physical sites.

IT-21 structure on the other hand, is a single AD forest per ship (multiple forests at the enterprise) to allow self-sufficiency when WAN connection is unavailable. Each ship carries its own forest root domain controllers to store domain-wide directory data (such as system security policies and user authentication data) and manage user-domain interactions, including user logon processes, authentication, and directory searches (Microsoft Technet, 2010).

Embarking units cannot get authenticated and authorized by the ship's DC as there is no trust between ship's domain and the ashore domains. An Embarkables forest,

including user accounts and all Embarkables objects, must be created and a two-way-trust established with the ship's forest in order access ship's local resources such as printers and to receive transport services via SATCOM.

This decentralized, multi-forest network management model, although more secure than a single AD forest, meets its purpose of providing data isolation and prevents network asset mobility or integration from any other domain.

Current Navy networks operate in different environments with unique requirements. They are not interoperable and therefore a seamless integration of assets from one network to another is not feasible.

5. How can the Navy Users Better and More Quickly Integrate Their Deployed Systems into Afloat Domains?

The author provides two recommendations for better and faster integration of ashore assets into the shipboard environment by (1) including an Embarkables test for all solutions prior to fielding to the operational environment, and (2) adapting existing solutions to provide "office like" services to embarking users.

Establishing the requirement to test ashore solutions on a simulated afloat environment will aid identify interoperability issues on a test atmosphere and have the issues resolved prior to deployment. Testing should simulate the integration of an NMCI or ONE-NET workstation into an IT-21 domain by testing the technical aspects as well as the process flow involved in the integration of the seat.

The second recommendation is adapting NMCI's DSTB to VPN to the home network for patches, security upgrades and policies, combined with the pre-position servers or the Airwing Embarkables servers for local network shared data and exchange capabilities, and establishing two-way-trust between the embarked unit domain and the ship's domain to access local resources such as printing, ship hosted applications and portals. Together, these solutions could potentially provide an "office like" experience to embarking users and workstations would be managed and maintained with latest OS and application patches by their own network, eliminating the need to reimage post deployment in order to reintegrate into the native network. An estimated cost of $228,621

to include initial DSTB procurement cost, monthly maintenance cost and technical support for six deployments in a four year period, could result in 3,800 man-hour savings and would minimize loss of data and loss of productivity by requiring minimal or no integration efforts to connect into IT-21 during deployments.

6. How can Seamless Access to Navy E-mail be Achieved?

Seamless e-mail is achievable by the implementation of a common Navy or DoD e-mail enterprise service architecture. A common e-mail enterprise service architecture would allow the access and exchange of electronic messages from anywhere in the world connected to the World Wide Web. Achieving a common Navy e-mail would require reengineering the current network and directory services architecture or moving e-mail to the 'cloud' by outsourcing e-mail services to a third party. Regardless of the selected approach, it will not be an easy undertaking and must be carefully evaluated.

Relinquishing control of military tactical and strategic data to a third party requires extensive risk analysis, especially for IA considerations and due to the inability to have full visibility of the network and security enforcements on sensitive and classified networks. Recognizing the cloud's dependency on the underlying network and how vital network survivability is for DoD mission, this risk would be a major area of consideration for DoD decision makers. Another consideration is the Navy's afloat unique SATCOM environment; low bandwidth and intermittent link will limit the access to exchange of data internally and externally.

Commercial technologies provide a hybrid models consisting of e-mail residing in the cloud and on-premise. This appears to be a more promising model if the intent for the government is to continue maintaining control of enforcing strict security policies while allowing more flexibility and mobility of user data, rather than transferring full control to a vendor. One of the hybrid models that is best suitable to support Embarkables is an architecture where some user mailboxes are on the cloud and some are on the on-premise servers. With this model, mailboxes can be moved from the on-premise servers to the

cloud for users on the move and during deployments; it allows scalability of size of mailboxes, such as smaller mailboxes for IT-21 users and other ashore users with limited need of e-mail usage.

Due to the uniqueness of DoD requirements, a tailored solution might be the right approach by applying commercial concepts on DoD internal networks to create "private" cloud offerings, enjoying many of the benefits of cloud computing such as more rapid and dynamic resource provisioning, but probably not resulting in the same economies of scale. This approach has been implemented by DISA providing a cloud solution for the Army. This ongoing pilot effort to exercise cloud technologies on real-world DoD networks is being closely watched by other services for future adoption across all DoD (Serbu, 2011).

C. CONCLUDING SUMMARY

The Navy has successfully delivered, operated and sustained IT networks to support DoD's mission and maintain communications superiority and dominance. These systems have advantages in reliability, maintainability, usability, supportability, and affordability characteristics but are deficient in other characteristics such as flexibility, adaptability, and portability.

Navy networks have become large complex systems with relatively stable architectures and no standardization of technologies or protocols, with variation of security requirements, and with a centralized acquisition and management entity. The outcome is a variation of network solutions resulting in interoperability challenges and degradation/loss of communication efficiency.

As DoD aligns systems and resources across organizations and military services, enterprise systems must be flexible, adaptable and reconfigurable. Whether developing new solutions or upgrading operational networks, system architects and engineers must implement a system-of-system approach and focus on developing dynamic reconfigurable system architectures (Williamson, 2012), with standardized protocols and technologies to enable adaptable and interoperable reliable systems to function anytime, anywhere.

APPENDIX: ASHORE NETWORK FUNCTIONAL DECOMPOSITION

4.0 Enterprise Application Support Services
4.1 Perform Briefing and Presentation Services
4.2 Perform Calculation Services
4.2.2 Calendaring
4.2.2.1 Manage Appointments
4.2.2.2 Shared Calendaring
4.2.3 Perform Scheduling Tasks
4.2.4 Perform Task Management
4.2.4.1 Maintain Address Book
4.2.4.2 Maintain Tasks
4.2.8 Manage Desktop Communication Applications
4.2.10 Conduct Instant Messaging
4.2.11 Perform Real-Time / Chat
4.2.12 Perform Real-Time Collaboration
4.2.13 Conduct Video Conferencing
4.2.14 Encrypt Data
4.2.15 Manage and Manipulate File and File Systems
4.2.15.1 Duplicate CDs
4.2.15.2 Perform Data Compression
4.3 Manipulate Documents
4.3.1 Convert Documents
4.3.2 Produce PDF Documents
4.3.3 View Documents
4.3.5 Perform Word Processing
4.4 Produce and Manage Audio and Graphic Media
4.4.2 Perform Desktop Publishing
4.4.3 Support Development of Graphics
4.4.4 Provide and Manage Clipart
4.4.5 Support Development of Presentations
4.4.7 Store and Retrieve Imagery
4.7 Data Management Services
4.7.1 Archive Data
4.7.2 Conduct Data Storage/Retrieval/Updating

- 4.7.3 Conduct Database Queries
- 4.7.7 Data Loading
- 4.7.10 Delete data
- 4.7.11 Maintain data integrity
- 4.8 Document Management Services
  - 4.8.1 Control Document Distribution
  - 4.8.3 Document Management

5.0 Enterprise System Services

- 5.1 Data Interchange Services
- 5.2 Control Operation of Computer
- 5.3 Provide Network Applications Services
  - 5.3.1 Determine Equipment Availability
  - 5.3.2 Determine Equipment Capability
  - 5.3.3 Determine Equipment Performance
  - 5.3.5 Disseminate operational/tactical information
    - 5.3.5.5 Manage user profile
    - 5.3.5.6 Provide directory services
  - 5.3.6 Exchange electronic mail
    - 5.3.6.1 Create and edit messages
    - 5.3.6.2 Receive messages
    - 5.3.6.3 Send messages
      - 5.3.6.3.1 Allow users to send e-mails to multiple users (cc)
      - 5.3.6.3.2 Allow users to send e-mails with hidden send lists (bcc)
    - 5.3.6.4 Manage Attachments
      - 5.3.6.4.1 Allow users to add file attachments to their outgoing e-mail
    - 5.3.6.5 Manage Inbox size
      - 5.3.6.5.1 Store incoming e-mail distinctly according to mailbox
      - 5.3.6.5.2 Store e-mail messages that have been sent
      - 5.3.6.5.3 Store incoming e-mail messages that have been read
    - 5.3.6.7 Manage Inbox e-mail folders
    - 5.3.6.8 Support Search capabilities
    - 5.3.6.9 Allow .pst creation
    - 5.3.6.10 Delete E-mails
  - 5.3.8 Provide network applications scalability
  - 5.3.9 Support web browsing
- 5.4 Provide Network Services
  - 5.4.2 Compress data

		5.4.4 Dynamically switch/route unicast (point-to-point), multicast and broadcast traffic across multiple networks						
			5.4.4.1 Identify potential data transmission paths					
				5.4.4.1.3 Establish connection-oriented network services				
				5.4.4.1.8 Maintain network-related information				
				5.4.4.1.9 Manage network operations				
					5.4.4.1.9.1 Automatically generate and display network status			
					5.4.4.1.9.2 Conduct performance management			
					5.4.4.1.9.3 Perform account management			
					5.4.4.1.9.4 Perform automated fault management			
					5.4.4.1.9.5 Perform dynamic configuration management			
						5.4.4.1.9.5.4 Manually configure/reconfigure the network		
					5.4.4.1.9.7 Perform network information assurance/security management			
						5.4.4.1.9.7.1 Authenticate user access		
						5.4.4.1.9.7.2 Ensure data/information confidentiality		
							5.4.4.1.9.7.2.1 Decrypt information/data	
							5.4.4.1.9.7.2.2 Encrypt information/data	
						5.4.4.1.9.7.3 Ensure non-repudiation		
						5.4.4.1.9.7.4 Maintain data file integrity		
						5.4.4.1.9.7.5 Prevent opportunity to attack		
					5.4.4.1.9.8 Perform technical control of network			
				5.4.4.1.10 Perform dynamic data transmission path selection				
					5.4.4.1.10.1 Establish redundancy in the network to avoid single-point failures			
				5.4.4.1.11 Provide network access scalability				
				5.4.4.1.12 Provide network services scalability				
				5.4.4.1.13 Synchronize network timing				
				5.4.4.1.14 Terminate network connection				
		5.4.5 Provide Networking Desktop Services						
			5.4.5.1 Provide Directory Services					
			5.4.5.2 Share Files and Printers					
			5.4.5.3 Provide File Transfer					
			5.4.5.4 Provide Message Services					
			5.4.5.6 Provide Remote Access					
	5.5 Provide Transport Services							
		5.5.5 Interface with Local/Wide Area Networks						
		5.5.6 Maintain appropriate level of security during data transmission						

		5.5.17 Access Control
		5.5.18 Role / Privilege Management
		5.5.19 User Management
		5.5.20 Data Verification
	5.6 Storage Management	
		5.6.1 Backup
		5.6.2 Data Archiving
		5.6.3 Enterprise storage resource management
	5.7 Manage Databases	

LIST OF REFERENCES

Burgard, J. (2011, June 15). ISEA Embarkable Staff Integration Team E-mail. San Diego, CA, USA.

Carey, R. J. (2010, March 09–11). *Connecting tha Naval Warfighting Team*. Redmond, WA, USA.

Defense Information Systems Agency. (2011, September 22). Defense Information Systems Agency Depatrment of Defense. Retrieved September 22, 2011, from Host Based Security System: http://www.disa.mil/Services/Information-Assurance/HBS/HBSS

Defense Information Systems Agency. (2010, January 25). *Host-Based Security System Concept of Operations*. Retrieved June 16, 2011, from PEO EIS Portal: https://www.peoeis.portal.navy.mil/ONE-Net/Engineering/ProjectsSolutions/Forms/AllItems.aspx?RootFolder=https%3a%2f%2fwww%2epeoeis%2eportal%2enavy%2emil%2fONE%2dNet%2fEngineering%2fProjectsSolutions%2fHBSS&FolderCTID=0x012000526DB822EBF25A4699F295C75A049BB7

Defense Information Systems Agency. (2009). *Host-Based Security System*. Dallas, TX: Hewlett-Packard Development Company.

Department of Defense. (2007). *Directive Number 8500.01E*. Washington, DC: Depatrment of Defense.

Department of Defense Manpower Data Center. (2010, September 30). *Active Duty Military Personnel Strengths by Regional Area and by Country*. Retrieved June 21, 2011, from US Department of Defense: http://siadapp.dmdc.osd.mil/personnel/MILITARY/history/hst1009.pdf

Department of the Navy Chief Information Officer. (2008). *Computer Network Defense Roadmap*. Retrieved May 16, 2011, from Department of the Navy Chief Information Officer Site. www.doncio.navy.mil/Download.aspx?AttachID=2334

Department of the Navy Chief Information Officer. (2006, December 30). *Information Assurance and Computer Network Defense Workforce Transformation*. Retrieved October 09, 2011, from Department of the Navy Chief Information Officer Site. http://www.doncio.navy.mil/PolicyView.aspx?ID=3057

Department of the Navy Chief Information Officer. (2008). *Naval Networking Environment (NNE) Strategic Definition, Scope and Strategy Paper*. Washington, DC: DON.

Department of the Navy PMW160. (2011, April 20). *Windows Server Update Services (WSUS) Concept of Operations*. Retrieved February 23, 2012, from Naval Networks Home Page: https://navalnetworks.spawar.navy.mil/

DXNET Training. (2009). Active Directory. *Lesson 4: Active Directory* . San Diego, CA, USA.

Embarkable Staff Integration Team . (2008). *ISNS Embarkables Models*. San Diego, CA: SPAWAR.

Enterprise Services Working Group. (2010, May 25). *Enterprise Services WG*. Retrieved June 10, 2011, from PEO C4I PMW160 Portal: https://nserc.navy.mil/

Federation of American Scientists. (2011). Federation of American Scientists. Retrieved December 11, 2011, from Executive Summary of the Commercial Satellite Communications (SATCOM) Report: http://www.fas.org/spp/military/docops/navy/commrept/index.html

Hewlett-Packard Development Company. (2010, September 08). *Deployable Site Transport Boundary*. Retrieved June 26, 2010, from NMCI Homeport: https://www.homeport.navy.mil/services/dstb/core/

Hewlett-Packard Development Company. (2011, February 16). *NMCI Core Build Contents*. Retrieved June 26, 2011, from NMCI homeport: https://www.homeport.navy.mil/services/

Hoang, V. (2011, December 13). HBSS. (N. Ramirez, Interviewer)

Kruse, H. (1995). *Data Communnications Protocol Performace on Geostationary Satellite Links*. Athens, OH: American Institute of Aeronautics and Astronautics, Inc.

LandWarNet. (2008, August 19–21). LandWarNet 2008. Retrieved October 04, 2011, from Armed Forces Communications (AFCEA) International: http://www.afcea.org/events/landwarnet/08/infoexchange.asp

Metz, T. F. (2006, October 31). U.S. Army Training and Doctrine Command. Retrieved November 15, 2011, from Guidance on Protecting Data At Rest (DAR): http://www.tradoc.army.mil/tpubs/misc/DAR/31%20Oct%2006%20-%20DAR%20Memo.PDF

Microsoft Technet. (2005, June 21). Microsoft Technet. Retrieved January 06, 2012, from Exchange Server 2003 and Active Directory: http://technet.microsoft.com/en-us/library/bb124887%28EXCHG.65%29.aspx

Microsoft Technet. (2009, January 22). Microsoft Technet. Retrieved October 16, 2011, from How Interactive Logon Works : http://technet.microsoft.com/en-us/library/cc780332%28WS.10%29.aspx

Microsoft Technet. (2010, March 16). Microsoft Technet. Retrieved January 15, 2012, from Understanding Transport in a Hybrid Deployment: http://technet.microsoft.com/en-us/library/ff645372.aspx

Microsoft Technet. (2011, June 1). Microsoft Technet. Retrieved September 13, 2011, from Active Directory Collection: http://technet.microsoft.com/en-us/library/cc780036%28WS.10%29.aspx#w2k3tr_ad_over_qbjd

Navy Marine Corps Intranet. (2010, July 01). *Continuity of Service Contract Statement of Work*. Retrieved 09 03, 2011, from SPAWAR Enterprise Public website: http://www.public.navy.mil/spawar/peoeis/nen/nmci/documents/attachment%201%20-%20statement%20of%20work.pdf

Navy Marine Corps Intranet. (2010, March 25). *Deployable Site Transport Boundary*. Retrieved June 26, 2011, from NMCI Homeport: https://www.homeport.navy.mil/services/dstb/

Navy Marine Corps Intranet. (2010, October 20). *Government Aid to Deploy v1.3*. Retrieved July 07, 2011, from PEO EIS Portal: https://www.peoeis.portal.navy.mil/ONE-Net/ONE-NET%20Deployables/Deployable_Team/Forms/AllItems.aspx

Navy Marine Corps Intranet. (2010). *Navy Active Directory Design*. Herndon, VA: Hewlett-Packard Development Company.

Navy Marine Corps Intranet. (2009, May 29). NMCI Contract N00024–00-D-6000. Retrieved October 16, 2011, from SPAWAR Enterprise Public website: http://www.public.navy.mil/spawar/PEOEIS/NEN/NMCI/Documents/Conformed%20Contract_Contract.pdf

Navy Marine Corps Intranet. (2005). *NMCI Deployables Support Plan*. Dallas, TX: Hewlett-Packard Development Company, L.P.

Net-Centric Geospatial-Intelligence Discovery Services. (2002). *Active Directory Naming Standards for COMPOSE & IT21 Block 1*. Washington, DC: DOD.

Podwoski, R. W. (2011). *Mobile Workstation Project - Technical Baseline*. San Diego, CA: SPAWAR.

Program Manager Warfare 160. (2011). *COMPOSE 3X Secuirty Patch*. San Diego,CA: SPAWAR.

Purhagan, D. (2010, November 21). ONE-NET EMS Lead Engineer. (N. Ramirez, Interviewer)

Rivera, J. (2009). Deployables STEAG Brief. Retrieved September 23, 2011, from PEO EIS Portal: https://www.peoeis.portal.navy.mil/ONE-Net/ONE-NET%20Deployables/Deployable_Team/Forms/AllItems.aspx

Rivera, J. (2010). Streamlined Embarkables. Retrieved September 23, 2011, from PEO EIS Portal: https://www.peoeis.portal.navy.mil/ONE-Net/ONE-NET%20Deployables/Deployable_Team/Forms/AllItems.aspx

Runyan, J. (2006). *NMCI-to-IT21 STEAG Brief for the Deployables Working Group (DWG)*. San Diego,CA: SPAWAR.

Schadler, T. (2009). *Should Your E-mail Live In The Cloud? A Comparative Cost Analysis*. Cambridge, MA: Forrester Research, Inc.

Serbu, J. (2011, May 4). All DoD eyes focused on Army's cloud e-mail transition. Retrieved November 26, 2011, from Federal News Radio: http://www.federalnewsradio.com/?nid=697&sid=2369712

Smith, T. (2003). *Interfacing IT-21 and BLII with NMCI*. San Diego: SPAWAR.

Space and Naval Warfare Systems Center. (2009). *Data At Rest Technical Design*. San Diego, CA.

Space and Naval Warfare Systems Center. (2010, January 10). *Deployable Application Architecture Overview*. Retrieved November 07, 2011, from PEO EIS Portal: https://www.peoeis.portal.navy.mil/ONE-Net/ONE-NET%20Deployables/Deployable_Team/Forms/AllItems.aspx

Space and Naval Warfare Systems Center. (2011, January 31). *ONE-NET Active Directory Technical Design*. Retrieved November 07, 2011, from PEO EIS Portal: https://www.peoeis.portal.navy.mil/ONE-Net/Engineering/ProjectsSolutions/Forms/AllItems.aspx?RootFolder=https%3a%2f%2fwww%2epeoeis%2eportal%2enavy%2emil%2fONE%2dNet%2fEngineering%2fProjectsSolutions%2fDirectory%20Services%2fActive%20Directory&FolderCTID=0x012000526DB822EBF25A4699F295C75A049BB7

Space and Naval Warfare Systems Center. (2010, August 05). *ONE-NET Data at Rest Pilot*. Retrieved November 04, 2011, from PEO EIS Portal: https://www.peoeis.portal.navy.mil/ONE-

Net/Engineering/ProjectsSolutions/Forms/AllItems.aspx?RootFolder=%2fONE%2dNet%2fEngineering%2fProjectsSolutions%2fDAR&FolderCTID=&View=%7b6C6A236B%2d4CFC%2d481E%2d940D%2d27D132F87044%7d

SPAWAR. (2011, April 25). *PEO C4I Products and Services*. Retrieved March 10, 2012, from SPAWAR Enterprise Public website: http://www.public.navy.mil/SPAWAR/PEOC4I/PRODUCTSSERVICES/Pages/default.aspx

U.S. Army. (2011, February 1). Virtualization.net. Retrieved January 20, 2012, from Army Enterprise e-mail moves to the Cloud: http://www.virtualization.net/1473-army-enterprise-e-mail-moves-to-the-cloud/

Washburn, D. (2011, July). Enterprise Services Mobile Workstation Project Brief. San Diego, CA, USA.

Weatherspoon, J. (2010, February 25). Streamlined Embarkables. Streamlined Embarkables Network Alignment OIPT Information Transport WIPT project IT2. San Diego, CA, USA: SPAWAR.

Williamson, R. (2012, January 21-11). *Model Based System Engineering (SoS) System of Systems/Enterprise Activity Introduction*. Retrieved February 10, 2012 from Object Management Group Portals: http://www.google.com/url?sa=t&rct=j&q=model%20based%20system%20engineering%20(sos)%20system%20of%20systems%2Fenterprise%20activity%20introductio&source=web&cd=1&ved=0CCoQFjAA&url=http%3A%2F%2Fwww.omgwiki.org%2FMBSE%2Flib%2Fexe%2Ffetch.php%3Fmedia%3Dmbse%

Wolff, R. (2008). *Deployable Site Transport Boundary*. Herndon, VA.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Mrs. Delores Washburn
   PEO C4I PMW-160
   San Diego, California

4. Mr. Julio Rivera
   PEO EIS PMW-205
   San Diego, California

5. Mr. Luis Ramirez
   SPAWARSYSCEN PACIFIC
   San Diego, California

6. Mrs. Mavis Machniak
   SPAWARSYSCEN PACIFIC
   San Diego, California